Doc ID: 6857247 Doc Ref ID: A2668312

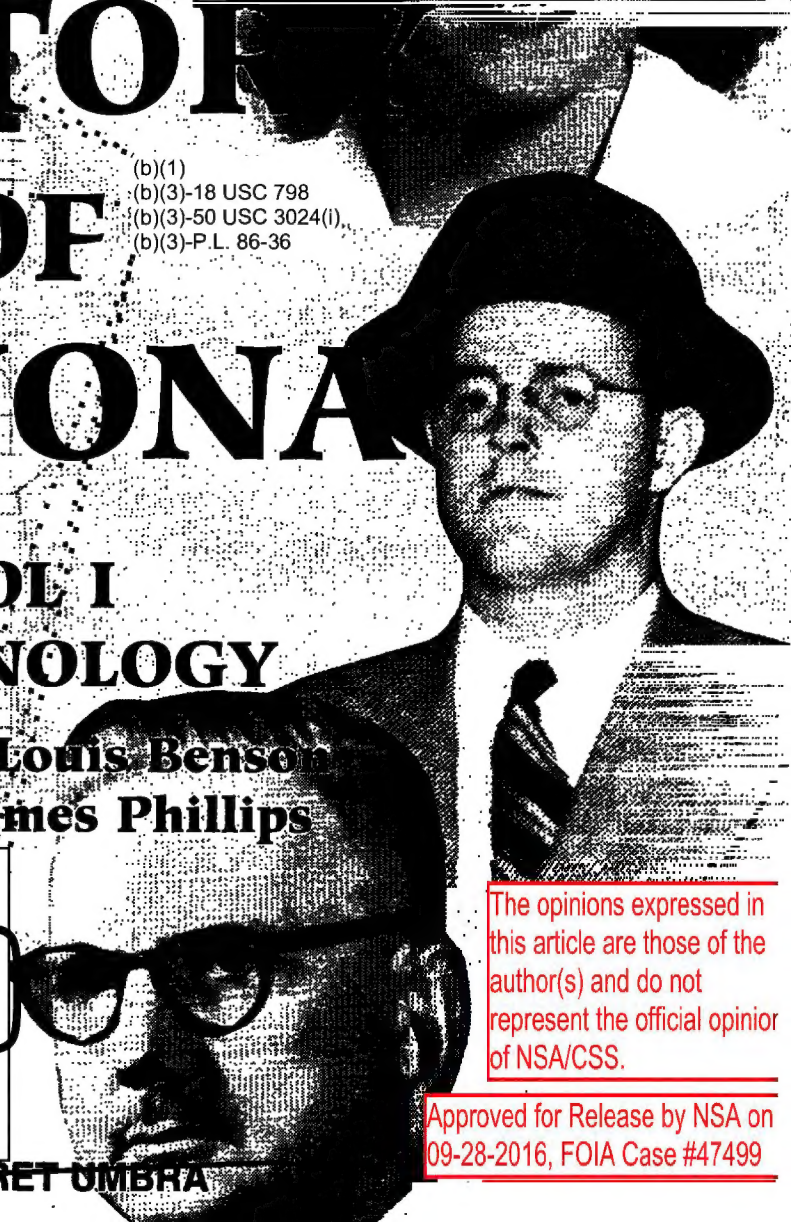
NATIONAL SECURITY AGENCY

HISTORY OF VENONA

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VOL I
CHRONOLOGY

By: Robert Louis Benson
Cecil James Phillips



Pages 67 - 98 are released in Document 3034869 / A701760
as released in FOIA Case 14255 on September 15, 2006

The opinions expressed in this article are those of the author(s) and do not represent the official opinior of NSA/CSS.

Approved for Release by NSA on 09-28-2016, FOIA Case #47499

NOTICE

THIS STUDY HAS BEEN COMPILED FOR CRYPTOLOGIC AND COUNTERINTELLIGENCE TRAINING, EDUCATION, HISTORICAL AND ANALYTICAL PURPOSES. IT IS PRIMARILY BASED ON SIGINT AND DOES NOT CONTAIN THE FULL STORY OF ANY ESPIONAGE CASE THAT MAY HAVE BEEN OPENED AS A RESULT OF THE SIGINT. IT IS NOT INTENDED NOR IS IT TO BE USED AS A BASIS FOR LEGAL OR ADMINISTRATIVE ACTIONS. SOME OF THE INFORMATION IN THIS STUDY IS UNRESOLVED FROM A LEGAL AND COUNTERINTELLIGENCE STANDPOINT: THE APPEARANCE OF A NAME IN KGB OR GRU TRAFFIC IS NOT TO BE TAKEN AS CERTAIN PROOF THAT THE PERSON WAS INVOLVED WITH THE RUSSIAN SERVICES IN A CLANDESTINE OR ILLEGAL WAY. SOME OF THE PERSONS IN THE TRAFFIC WERE PUBLIC FIGURES WHOSE LOYALTY HAS NEVER BEEN IN QUESTION. OTHERS COULD HAVE BEEN, AT SOMETIME, COOPERATING SOURCES ASSISTING THE FBI OR OTHER US/ALLIED SERVICES. A NUMBER OF IDENTITIES HAVE BEEN WITHHELD.

UNLESS OTHERWISE ATTRIBUTED, OPINIONS EXPRESSED IN THIS STUDY ARE THOSE OF THE AUTHORS.

March 1995

FOREWORD

I am pleased to release this history of Venona to a still necessarily limited readership in NSA and the intelligence communities in the U.S. and the U.K. Over the years there have been a number of efforts to document this historic event. Now, finally we have it through the exceptional efforts of Lou Benson, a career employee of the NSA Office of Security (M5), assisted by Cecil Phillips, a colleague who long ago as part of a small team at Arlington Hall, made the fundamental breaks into the KGB and GRU ciphers. Cecil, along with Gene Grabeel, Genevieve Feinstein, Frank Lewis, Dick Leibler and a handful of others paved the way for the brilliant book-breaking of Meredith Gardner which revealed the massive Soviet espionage against the United States and Great Britain. Gardner's work led to the splendid CI exploitation headed by Bob Lamphere of the FBI, and to the involvement of GCHQ, British Security Service and CIA.

On a personal note I am proud to have made a small contribution to the Venona effort during my time in the old A77. Even back then, in the middle 1970s, I believed that the history of Venona had to be written to show the magnificent work of NSA and its predecessors and to show the role of Sigint in supporting national counterintelligence and indeed the strategic interests of our country.

I urge readers of these volumes to put to use, today, the lessons of this complicated story so well told by Lou Benson and Cecil Phillips.

William P. Crowell
Deputy Director, NSA

~~TOP SECRET UMBRA~~

(b)(3)-P.L. 86-36

BACKGROUND

In about 1981, I first had the idea to write a history of Venona[1] — my plan was to work at it in the evenings and the occasional weekend. I talked to [redacted] then Chief of [redacted], the NSA element that had run the Venona program. Jack did not agree that this should be done; he said the matter was too sensitive, and in any case I could not convince him that I, a member of the NSA Office of Security, was the person to do the job. Over the years I made a few more offers to write the history but had no success.

In May 1991, I tried again and this time had success. [redacted], Chief of [redacted] and Bill Crowell as Chief of Staff and then DDO (and now D/DIR) were enthusiastic and supportive. Bill said the history needed to be done to show the extraordinary accomplishments of NSA and its predecessors. He also said that we needed a detailed history, "on the shelf, ready to take off" when the time and audience were right.

Stuart Whittle, one of the first persons I interviewed, told me that I needed to talk to Cecil Phillips before I did anything else. That was very good advice, and Cecil and I worked the project jointly from June 1991 to June 1993.

I wrote almost all of this three volume history. Cecil provided technical papers for me to use, and he completely wrote some of the technical sections. We did many interviews together. Most important, Cecil had joined the Russian Dip problem on May Day 1944, and he had almost perfect recall of people and events of the 1940s and early 1950s. He often remembered exact dates and circumstances. This history really could not have been written without him.

Robert Louis Benson

[1] Venona is the third name used to describe these translations. Previous names were: Drug and Bride.

~~TOP SECRET UMBRA~~

ACKNOWLEDGEMENTS

National Security Agency

Bill Crowell, Deputy Director
[redacted] former Deputy for Administration
[redacted] former Director of Security
Dave Gaddy, former Chief, Center for Cryptologic History
Dave Hatch, Chief, Center for Cryptologic History
[redacted] Office of Security
[redacted] Office of Security
[redacted] Office of Security
[redacted] Office of Security
[redacted]
Stuart Whittle
[redacted]
[redacted] NSA Archives
[redacted] NSA Archives
[redacted] NSA Archives
[redacted]

(b)(3)-P.L. 86-36

(b)(6)
(b)(7)(C)
OGA

Federal Bureau of Investigation

[redacted]

FBI

Government Communications Headquarters (GCHQ)

Sir Peter Marychurch
Geoffrey Sudbury
Howard Vincent
Lou Maddison
David Long
Shawn Massey
Alec Hobart

ACKNOWLEDGEMENTS

Former Arlington Hall, NSA and Intelligence Community Personnel

Frank Rowlett
Ferdinand Coudert
Oliver Kirby
S. Wesley Reynolds (FBI)
Robert J. Lamphere (FBI)
Bob McCaslin (FBI)
Gene Grabeel
Dr. Samuel Chew
Mildred Hayes
Dr. Louis Tordella
Arthur Levenson
Ann Caracristi
Dr. Richard Leibler
Alice Sachaklian
Sam Snyder
[redacted]
Katy McDonald (b)(3)-P.L. 86-36
[redacted]
Gloria Forbes
Mary Boake
Bill Kulp
Carrie Berry
[redacted]
Paul Deafenbaugh
Ruby Caporaletti
Janice Cram
Angeline Nanni
Louise Prather

VENONA

VOLUME ONE

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

I. INTRODUCTION 1

A. Problems of Terminology 1
B. Venona 1
C. Scope of This Study and Sources 3
D. Sources 4

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943 8

A. February 1943 8
B. The Traffic 8
C. Interlude: The Sinkov Mission to the UK 11
D. The Decision to Begin the Russian Problem 12
E. The Beginning of the Russian Problem at Arlington Hall 13
F. The Russian Problem Put on Ice 16
G. The Russian Program Resumed 17
G.1. Recruiting People for Arlington Hall (19)
H. Russian Military Traffic 1943–44 20
I. More Japanese Military Attache Messages 22
J. Progress on Russian Dip 24
K. UK Work on the Russian Problem 1930s–1944 29

III. THE BILL SMITH ERA – NOVEMBER 1943–1946 33

A. Change of Command 33
B. Developments During 1944 34
C. Lauchlin Currie, the Silvermaster Ring and the KGB: Spring 1944 36
D. May Day 1944 38
E. Carter Clarke Delivers a Warning to Arlington Hall 42
[redacted] 43
G. Slow But Steady Progress at Arlington Hall and Nebraska Avenue 1944–1945 46
H. TICOM and BOURBON: US–UK Joint activities in 1945 49
I. Gouzenko, Bentley, Chambers and the Anonymous Ltr. 61

IV. THE VENONA BREAKTHROUGH 67

A. Arlington Hall in 1946 67
B. The Venona Breakthrough of December 1946 68
C. Covernames, the FBI and the British 73

V. RUSSIAN DIP 1945–1949: THE PROCESS AND THE PEOPLE 93

A. Overview 93
[redacted] 93

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~TOP SECRET UMBRA~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VENONA – TABLE OF CONTENTS

[redacted] 94
[redacted] 94
D.6. The Players in the Reading Game (97)
E. Book Breaking and Publication 97
F. Summary 98

VI. US–UK PROGRESS 1948–1952 99
A. ASA–GCHQ Cooperation During 1948 and 1949 99
B. Black Friday — 20 December 1949 103
C. Meredith Gardner's Translations of KGB Traffic 104
D. Lamphere's Covername Study and CI Progress 108

VII. BILL WEISBAND AND KIM PHILBY 113
A. Introduction 113
B. Wes Reynolds Alerts Carter Clarke about Weisband 113
C. The Weisband Espionage Case: The Torn Photo of Shirley Temple 115
C.1. Weisband in New York 1920s–1941 (117)
D. Information From Analtoli Golitzyn 118
E. Weisband in ASA and AFSA 1943–1950 119
F. Russian Systems Possibly Compromised by Weisband 127
G. Is Weisband in the Venona Traffic? 132
H. The Weisband Case in Later Years 137
I. Kim Philby and Arlington Hall: Background 139
J. HOMER and Philby 140
K. Philby in Venona 145

VIII. VENONA DEVELOPMENTS DURING THE 1950s 149
A. Discussion 149
[redacted] 149
[redacted] 151
[redacted] 152
[redacted] 153
F. The CIA 160
G. Covernames and Identifications 160
H. Some Operational and Organizational Highlights 161
I. The Later 1950s and Early 1960s 164

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~TOP SECRET UMBRA~~

VOLUME TWO

IX. THE VENONA DECRYPTS: INTRODUCTION, FACTS AND FIGURES 167
A. Introduction to Volume Two 167
B. Venona Facts and Figures 168
C. Translations, Covernames, and the Problem of Naming Names 170

X. ALGER HISS. KGB COVERNAME : ALES 175
A. Background 175
B. Hiss in Venona 175

XI. THE ROSENBERGS AND THE ATOMIC BOMB SPY RINGS 183
A. Introduction 183
B. The Rosenbergs and Greenglasses 184
C. The Rosenbergs in Venona KGB Covernames (for J. Rosenberg): ANTENNA, LIBERAL 186
D. Other Atomic Bomb Spies in Venona 196
E. Comments 208

XII. HARRY DEXTER WHITE. KGB COVERNAMES: JURIST, LAWYER, RICHARD 209
A. Background 209
B. Harry White in Venona 210

XIII. NEW YORK KGB: AGENT NETWORKS, TRADECRAFT AND SECURITY 221
A. Introduction 221
B. Internal Security 221
C. The New York Residency 233
D. Some Problems in Running the New York Residency 236
E. The Agent Networks 243
F. "We propose handing over..." : Network Control and Operations 247
G. Communist Party Liaison: Bernard Schuster (ECHO, DICK) 252
H. A Three Way Struggle for Control: MAJ – ALBERT – ROBERT 256

XIV. NEW YORK KGB: RECRUITING, GENERAL TRADECRAFT AND INTELLIGENCE COLLECTION 271
A. Introduction 271
B. Agent Recruiting 271
C. General Tradecraft 278
D. Intelligence Reporting and EEI 291

XV. THE TRUE BELIEVERS: JUDITH COPLON (COVERNAME: SIMA) AND FLORA WOVSCHIN (COVERNAME: ZORA) 307
A. Background 307
B. The Venona Traffic 308

VENONA – TABLE OF CONTENTS

XVI. DUNCAN LEE AND KGB PENETRATION OF U.S.INTELLIGENCE AGENCIES 317
A. Overview 317
B. Penetration of Military and Naval Intelligence and the FBI: the Venona Record 318
C. KGB Penetration of the OSS (KGB Coverterm IZBA = OSS) 325

XVII. THE WHITE HOUSE 349
A. Introduction 349
B. "KAPITAN's Wife" 349
C. Who Was the Covername Known as "19"? 355
D. KGB Covername PAZh — Lauchlin Currie? 359
E. Bribery and a White House Official 362
F. Covername MOLE: Some KGB Assets with Access to Congress and the Democratic Party 363
G. Presidential Analyses by the KGB 366
H. More References to High Level Penetrations and Connections 370

XVIII. KGB SPECIAL OPERATIONS IN THE U.S. AND MEXICO 373
A. Introduction 373
B. The KOMAR/GNAT Affair: KGB NY Looks for a Defector 373
C. The RITA/GNOME Case: The KGB Tries to Spring Trotsky's Assassin 381
D. Other Mexico City Operations 401

XIX. THE MEDIA 415
A. Introduction 415
B. Some Journalists 415
C. The KGB Runs a Record and Music Company in Hollywood 427
D. Other KGB Activities in Hollywood 432
E. Broadcasting and Books 436
F. The GRU and the Media 438

XX. THE KGB IN SAN FRANCISCO 441
A. The Traffic 441
B. KGB SF Intelligence and Tradecraft Messages 442
C. Security Countermeasures at the San Francisco Residency 451
D. The Fifth Line of the KGB: Security of the Merchant Fleet 455

VOLUME THREE

XXI. THE GRU 469

A. Introduction 469
B. The Traffic and Cryptanalytic Difficulties 469
C. Washington <–> Moscow GRU Messages 472
D. New York GRU Messages to Moscow 474

XXII. THE GRU – NAVAL 493

A. Introduction and Traffic Statistics 493
B. The Russian Naval Attache in Washington 494
C. Agent Operations and Tradecraft 502
D. SALLY/AUSTRALIAN WOMAN – GRU Naval Lands an Illegal 512
E. News From Home 522

XXIII. THE VENONA PROGRAM IN THE 60s and 70s: AMINISTRATION, CRYPTANALYSIS AND INTELLIGENCE 525

A. Discussion 525
B. Administration 525
C. Cryptanalysis 529
[redacted] 532
E. The Final Effort — the Venona Program in the 1970s 534

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VENONA – TABLE OF CONTENTS

APPENDICES

APPENDIX ONE – GLOSSARY 541

APPENDIX TWO – THE ANONYMOUS LETTER OF 1943 547

APPENDIX THREE – COUNTS OF AVAILABLE KGB AND GRU MESSAGES 551

APPENDIX FOUR – U.S. PEOPLE WHO WORKED ON VENONA 557

APPENDIX FIVE – SECURITY OF THE U.S. VENONA PROGRAM 559

APPENDIX SEVEN – ADDITIONAL IMPORTANT MESSAGES 567

APPENDIX EIGHT – KGB AND GRU MESSAGES LONDON <–> MOSCOW 1940–41; 1945–46 571

APPENDIX NINE – THE ADDITIONAL KGB WASHINGTON TO MOSCOW MESSAGES, 1945 581

APPENDIX TEN – THE HOMER/GOMER MESSAGES 587

APPENDIX ELEVEN – GENERAL SUDOPLATOV AND VENONA 597

APPENDIX TWELVE – CLARIFYING WHAT MADE VENONA POSSIBLE 601

VENONA

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

I. INTRODUCTION

A. Problems of Terminology

This historical study carries a burden of anachronistic terminology, starting with the key word in the title—VENONA. The term Venona only came into use in the 1960s, the fourth, depending how one counts, codename for the US–UK exploitation of high grade Soviet intelligence service communications. Furthermore, the most spectacular breakthroughs occurred before a codename was regularly put on product reports of this type. The term Classical [redacted] (for Russian Diplomatic) might be preferred, but Venona has now widely appeared in open sources. Then we have the problem of organizational designators for both sides, and now even the matter of naming the opposition country. The term Venona will generally be used with the earlier codenames introduced if required by the context e.g. for quotations from US–UK documents. Those earlier codenames were: JADE, BRIDE and DRUG.

KGB and GRU will be the exclusive designators for the opposition services—the entities whose communications we exploited—except that NKVD will be used when the reference is to the militarized or police elements of the state security apparatus.

For our side the matter of organizational designators is more difficult, because we devote a great deal of attention to the very early years of the Russian problem, taking care to describe in some detail who did what, when. Therefore, the contemporary and often changing names for the U.S. organizations will sometimes be used.

B. Venona

Venona is the most recent code name for the US–UK exploitation of encrypted KGB and GRU communications of the period 1941–48. Except for one lane, Canberra—Moscow, none of the traffic was read until long after the messages had been sent. Venona was not a real-time or near real-time operation. New York KGB messages of, for example, 1944 or 1945 were not first read until December 1946 (one message) and 1947. The greatest period of decryption and translation, at least for KGB messages on the U.S.—Moscow lanes, occurred in 1948-mid 1950s, and mostly involved KGB messages sent in 1944 and 1945. As we will describe, the Venona exploitation program ran until September 1980, the last published translation being a KGB message that had been sent in 1943.

Several points made here will be built upon and repeated throughout the study.

For many years the ASA–AFSA–NSA cryptanalysts worked the Russian Diplomatic problem as a whole, attacking both current messages and accumulated back traffic. The material that came to be known as Venona, imbedded in that Diplomatic traffic, comprised only a small minority of the whole. Trade messages—ultimately designated as [redacted]—were highest in volume. These Trade communications, sent in diplomatic channels, concerned Lend Lease information and reports to and from the Soviet Government Purchasing Commission: an immense volume of information about equipment, parts and other supplies needed by and being sent to Russia to assist in the war against Nazi Germany. True Diplomatic, essentially Consular messages, later called [redacted] passed between the US–UK and the Soviet Foreign Ministry. What we know as Venona also passed on Diplomatic links:

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

I. INTRODUCTION

- KGB (known to US–UK as [redacted] or [redacted]
- GRU (known as [redacted] or [redacted]
- GRU-naval (known as [redacted] or [redacted]

The Trade messages bore the address of the Trade Ministry; all the other systems, including the intelligence service messages, that of the Foreign Ministry, or at the US–UK end, the embassy or consulate. The true identity of the communicants was concealed by cipher. Each Russian entity had its own unique codebook. In attacking all these systems simultaneously, the US–UK followed two points of doctrine, the first an absolute cryptanalytic necessity, the second a matter of cryptanalytic optimism:

- First, from the similarities of cryptographic indicators and other message externals, it became clear early on that all classes of so-called Russian Dip should be worked together to find the best messages to attack. As we shall see from the results obtained, if a cipher pad used for routine Trade messages could be matched with an identical cipher pad used by the KGB, then a so-called "depth of two" existed and the messages might be read. (The actual text of the Trade message would be of no interest.)

- Second, the UK and the US had had tremendous, virtually 100% success against German and Japanese high grade ciphers, both machine and manual, during World War II—the German Enigma and the Japanese Purple machines for example. The U.S. had even broken a German diplomatic one–time pad system. Our cryptanalysts therefore remained optimistic that high grade Russian diplomatic systems (and military) would also fall. For that reason [redacted] Many of the high level military systems were entered fairly quickly as we had hoped—and then lost quickly because of probable espionage at ASA (a case we will discuss at length).

The Venona project, then, remained frozen in time. Russian traffic of 1942 to 1946 (rather little on each end) could be exploited but that was all. The Venona cryptanalyst of 1948 could read KGB messages of 1944; in 1980, the Venona cryptanalyst was still exploiting that same block of exploitable traffic that had been sent in the 1940s. But if the US–UK analysts [redacted] the Russians couldn't very well get back the earlier traffic that could be exploited. They had to wait—or make emergency moves as in the case of Burgess and Maclean—as their spies were identified.

A few words on Russian cryptographic systems and myths relating to them. The Venona traffic passed on both international commercial radio circuits and national links. The communications were encrypted by first using the values in a code book and then enciphering those numbers from one–time pads, that is, by taking the numbers from the pads and adding them to the numbers from the code book. Such a system could not be broken unless the cryptanalyst possessed the one–time pads (of which there were hundreds of thousands) or knew the precise means of pad generation (that is, how the numbers in the pad had been selected) and could replicate it. A third possibility remained: the key in the pads might be somehow misused or re-used and thus lose their uniqueness. That was our opening into Venona.

As for the myths, the so-called "Black Friday", 20 December 1949 was not a Friday, and is an event of no real significance to the US–UK cryptanalytic effort on Venona or Venona related materials. Likewise the Venona breakthrough did not come about because the OSS had obtained Russian codebooks. The OSS did not in any way contribute to the Venona break; the fundamental cryptanalytic discoveries and the decryptions through 1952 were not aided by our side having any KGB or GRU code book from any source. It was an analytic success. The story of the capture of Russian cryptographic material is an interesting one and will be told in some

detail. But the benefits from those actions came later in the Venona story (and to repeat, had nothing to do with the OSS).

C. Scope of this Study and Sources

Much of this study will be non–technical. However, significant technical information will make unannounced appearances throughout the text, written by Cecil Phillips, one of the founders of the Venona program.

In the course of this study, the term "I" usually refers to Benson, the principal author of the study; and "we" may refer to Benson and Phillips or merely the form suggesting a partnership between author and reader.

The study contains three major themes, or perhaps we should say, the histories of three different aspects of Venona:

1. U.S. exploitation of the Venona material, at ASA, AFSA and NSA, with emphasis on the earlier years (1943–1954) but including the entry of the FBI, CIA and GCHQ onto the problem.

2. KGB and GRU espionage, tradecraft and special activities in the U.S. (and Mexico) as revealed in the Venona decrypts—case studies, examples.

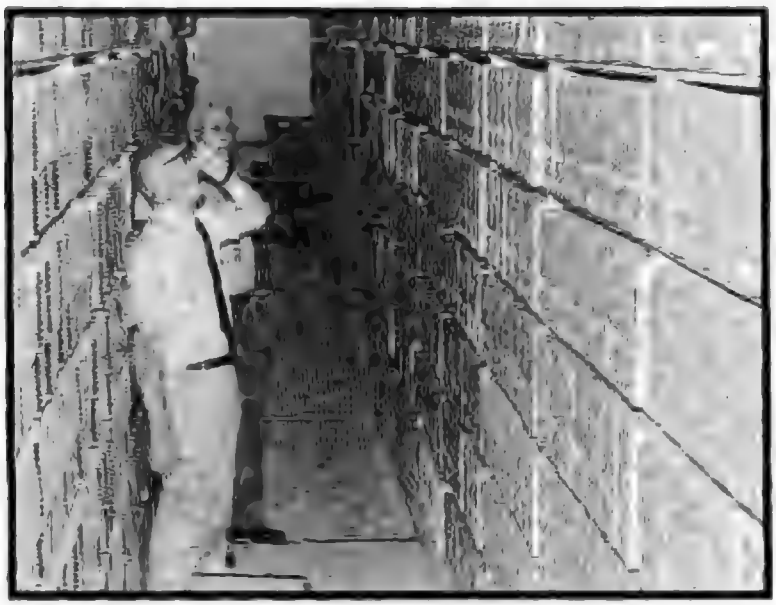
3. KGB espionage against the Venona effort.

This study emphasizes the U.S. Venona experience, but with, I hope, considerable attention to the fact that Venona exploitation became a US–UK partnership. This study would have been difficult to write without the UK documentary sources held in the NSA Venona collection.

This study should be considered a source book. It is not the history of U.S. counterintelligence or Russian espionage. Often, usually in fact, I have not put a case in full context—we are after the Venona part of the record, often to the exclusion of the rest of the story. On the other hand, I have in some cases gone rather far afield. Sometimes this is a matter of preference.

In authorizing, and indeed commissioning this study, Bill Crowell, as NSA Chief of Staff and then DDO, said it was time that we put together the NSA view of Venona, to have on the shelf, ready to take out and show to the appropriate audience, the story of an exceptional undertaking by this agency and its predecessors.

I. INTRODUCTION



◀ Cecil Phillips (foreground) and Lou Benson in the Venona Collection.

Cecil Phillips and Bill Hawkins examining a Venona cryptanalytic worksheet. ▶

(b)(3)-P.L. 86-36

D. Sources

The sources for this study include four major archival collections:

1. The Venona Collection. Held in the NSA archives and records center, having been preserved and sent there by Mildred Hayes, and then inventoried and protected by Bill Hawkins, this is the most important collection: the four boxes of Venona translations, the 700,000 messages held in 1391 Shinn boxes, the [redacted] cryptanalytic worksheets and the 200 boxes of everything else: FBI and CIA reports, logs, code books, TICOM

material, technical reports, GCHQ papers, correspondence and etc. (note the amount of material that went into the production of just four boxes of translations).

2. The NSA Archives. This was a major source for early papers on the Russian problem, TICOM papers, and for organization charts and photographs.

3. The archives of the NSA Center for Cryptologic History. Again a major source for the early history of the Russian problem, containing papers of exceptional interest and importance such as the Sam Snyder diaries and the many volume history of the SSA (The U.S. Army's Signal Security Agency).

4. Counterintelligence papers of the NSA Office of Security.

Cecil Phillips and I, jointly or independently, conducted many interviews of Venona veterans including the two people who started the Russian problem in 1943 and the person who turned out the lights on Venona in 1980. I conducted a number of interviews at GCHQ, and interviewed UK Venona veterans visiting the U.S.

On occasion I do not cite a source when it might seem appropriate, and a few times the source seems to have been obscured. This is intentional.

I. INTRODUCTION

(THIS PAGE INTENTIONALLY LEFT BLANK)

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

Gene Grabeel, who founded the U.S. Russian SigInt program on 1 Feb 1943 (1942 photo).

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

A. February 1943

The Russian Sigint problem began on Monday, 1 Feb 1943, in great secrecy and with minimum resources — just two people, Miss Gene Grabeel and 2/Lt Leonard M. Zubko, both recent arrivals at the Army Signal Security Agency, Arlington Hall Station, Virginia. Lt. Zubko, a 1942 graduate of Rutgers University (BSME) came to Arlington Hall after completing the Infantry School at Ft. Benning. He did not know what to expect and had never heard of the place. As a combat arms officer anxious to command troops, he was surprised to find that Arlington Hall seemed to be staffed entirely by female civilians.[1] Though he never knew for sure, he assumes that he got the assignment to Arlington Hall because he was an engineer, and the Russian assignment, several months later, because he knew the language (his parents had come from the Ukraine).

Gene Grabeel's assignment to the Russian problem was even more unlikely. After graduating from Longwood College in Farmville, Virginia, she taught at the high school in Madison Heights, near Lynchburg, Virginia. She did not like teaching. In Fall 1942 (in her second year as a schoolteacher) she asked her father what he thought about her taking a job with the federal government. He encouraged her to "go to Washington for six months and shuffle papers." In early December she talked to Lt. Paavo Carlson, a young Signal Corps officer who was recruiting civilians at the Post Office in Lynchburg. He offered her a position with the Army in the Washington area, but would not tell her what she would be doing. He asked her to leave for Washington the next day. Miss Grabeel accepted the position but told Lt. Carlson that she needed a little time to find a replacement teacher. On Sunday, 28 December 1942, she arrived in Washington, took a taxi to Arlington Hall and reported to the duty officer. Four weeks later she and Lt. Zubko started the Russian problem.[2]

Major Frank Rowlett, a friend and neighbor of her family in Virginia, and a senior officer at Arlington Hall, took her to meet Lt. Zubko. Rowlett told them to observe the strictest secrecy, and not to discuss their project with co-workers. Otherwise she received no particular instructions on how to begin or anything about the nature of the target.

Miss Grabeel and Lt. Zubko went to work. They sat at two tables in one corner of a room, the only other occupant being Major Geoffrey Stevens, the British liaison officer at Arlington Hall who had a desk in another corner. This curious and perhaps accidental arrangement may have led to some difficulties, for at that time and indeed for the next two years, the Army did not share with the British even the "fact of" the U.S. Sigint effort against Russia. Miss Grabeel and Lt. Zubko began by sorting back traffic by lane and date, looking for ways to categorize the material by system and user. Arlington Hall held a considerable body of Russian traffic (variously estimated as several or 6 to 8 filing cabinets full), and as the matter of coverage and the search for back traffic forms a significant part of the Venona story, we now consider what was available to the U.S. up to Feb 1943.

B. The Traffic

The Signal Security Agency's predecessor organization, the Signal Intelligence Service, acquired a dedicated intercept unit in Jan 1939, namely the Second Signal Service Company (later battalion) which operated several monitoring stations (MS) in the pre-war period including:

---

[1]Zubko, telephone conversation, 18 March 1992. The Signal Security Agency, re-named the Army Security Agency in 1945, eventually employed more than 5000 women. The women employees worked a wide range of duties, from clerical to crypto-linguist. WAC enlisted personnel had a major role in intercept operations, especially at the SSA field site at Two Rock Ranch, California, the principal site for the collection of Japanese Army mainline traffic.

[2]Grabeel interviews, 15 Oct 1991 and 10 March 1992 at Blackstone, Virginia; first interview by Robert L. Benson, second by Benson and Cecil Phillips. Carlson did not recall recruiting Miss Grabeel but has vivid memories of the recruiting campaign.

MS–1 Ft. Monmouth, NJ
MS–2 The Presidio of San Francisco
MS–3 Fort Sam Houston, Texas
MS–4 Quarry Heights, Canal Zone
MS–5 Fort Shafter, Hawaii
MS–6 Fort McKinley, Philippine Islands
MS–7 Fort Hunt, Virginia

These were fairly modest operations, for example, the Fort Sam Houston operation staffed by 11 enlisted men; the Fort Hunt site by one officer and 25 enlisted men (these are sample figures from 1939–41; the numbers and sites changed from time to time). Before establishing the Second Signal Service Company, the Army had relied on various other ad-hoc and often changing intercept arrangements. For example, in an early experimental operation—a hearability study and traffic sampling—the Provisional Radio Intelligence Detachment at Ft. Monmouth, commanded by Lt. Mark Rhoads, logged 381 foreign diplomatic messages from 1 Oct 1933 to 1 July 1934, including 63 Russian diplomatic messages.[3] Regular U.S. intercept of Russian diplomatic traffic, which contained KGB and GRU communications (though of course this was unknown to the U.S. at the time) began in 1939 as part of a general effort against all or most foreign diplomatic communications passed on international commercial circuits. The Army Signal Intelligence Service did not attempt a cryptanalytic attack on the Russian traffic but put it aside for future study.[4]

However, at the risk of pushing this study ever further back in time and away from Venona, we must note that during the 1920s and up to 1932, the Signal Intelligence Service had unsuccessfully attempted to break Russian diplomatic systems. The major effort took place in 1930–31 when Congressman Hamilton Fish, as chairman of the House Committee on the Investigation of Communist Propaganda, subpoenaed copies of Amtorg Trading Corporation messages held by U.S. cable and telegraph companies. He turned these over to the Navy for analysis and the Navy, unable to break into the messages, passed them along to the Army. No luck there either. It is worth quoting some comments made to G–2 in Feb 1931, by Major D.M. Crawford, head of the Signal Intelligence Service:[5]

> *Judging by what is known of Russian cryptographic methods in general, the (Russians) are employing complicated, scientifically constructed systems designed to resist the organized efforts of expert cryptanalysts. It is my belief that half-way measures and sporadic attempts will get nowhere in this case; nothing short of deep, long continued, and painstaking analysis has any chance of leading to a successful solution.*

The Venona story indeed!

While U.S. cryptanalytic and translation resources had to be concentrated on the highest national priorities of the time—Japan, Germany and Italy—collection procedures allowed for a vacuuming up approach. From 1939 to 7 December 1941, we find that encrypted Russian diplomatic traffic was taken in a modest amount from two principal sources: intercept of commercial circuits (that is foreign government traffic sent and received by, for example, RCA), by Station 3 at Fort Sam Houston — which seems to have had the principal responsibility

[3]"History of SSA in World War II", Volume XIII, Part I, 1945. Center for Cryptologic History (CCH), IV.B.1.13

[4]Interview of Frank B. Rowlett, by Benson, 14 Jan 1992, Sarasota, Florida.

[5]"Data on Soviet Cryptographic Systems 1917–33", Signal Security Agency, 15 May 1945. CCH Collection, III.O.22. See especially pages 14–15.

for copying the Russian traffic; and clandestine photography of Russian messages filed at the U.S. cable companies.

The clandestine photography procedure originated in an arrangement between the Army Signal Corps and David Sarnoff, chief executive officer of RCA and a reserve Signal Corps officer. In January 1940, Mr. Sarnoff wrote the Adjutant General accepting a War Department proposal to have a Signal Corps officer assigned to RCA for six months, "to pursue a course of study." As Earle F. Cook (Major General, retired) would recall "All of this nonsense was a cover — looking over the traffic was what I was there for."[6] With the cooperation of RCA, who provided a safe room and photo equipment, diplomatic messages were photographed and delivered to the Signal Intelligence Service. While Cook describes the Washington DC operation in some detail, we know that similar photo operations took place in New York City and possibly San Francisco. Photography meant perfect copy of the message as sent and allowed coverage of traffic that had not been intercepted or could not be (the Army copied manual and high speed morse but not printer).

Earle F. Cook. "Looking over the traffic was what I was there for"

A sampling of KGB (and some GRU) traffic from 1940 until 7 Dec 1941 on U.S.<—> Moscow lanes shows that both intercept and photography were extensive, but the coverage erratic. KGB New York traffic was intercepted by Station 3, mostly, but also by Stations 4 and 7 (Canal Zone and Fort Hunt, VA respectively) throughout 1941, while the photography mostly took place in January and again during the last few months of that year. Washington <—> Moscow GRU was collected by both means, especially for January–August 1941. Only a small amount of Russian intelligence traffic to and from San Francisco and Los Angeles seems to have been taken. The KGB did not communicate out of Washington until 1943 (the New York City Residency serviced the KGB station in Washington).

The KGB and GRU traffic represented a minority of the Russian messages sent and collected — the bulk of the material then and later would be Trade and Consular.

[6]NSA interview of General Cook, 15 July 1982, by Robert D. Farley, OH 14–82, CCH Collection. See also the interview of Colonel Robert E. Schukraft, 2 Oct 1980 by Bob Farley, OH 36–80. These interviews are extraordinary sources of information about Army Sigint.

The Army and Navy discussed the collection and processing of Russian traffic in some of their pre-war negotiations on coordination. From July–Oct 1940 several committees met to discuss a division of overall U.S. intercept effort, especially of diplomatic communications. The Army, or at least General Mauborgne, the Chief Signal Officer, preferred to divide the intercept coverage based on the transmitting station. The Navy preferred a more comprehensive scheme based in part on target entity, but eventually agreed to the Army proposal, though with the interesting proviso that the Army would turn over to the Navy all Russian traffic.[7] A small Navy effort against Russian diplomatic, begun in 1938 and which perhaps continued into 1941, produced no results and did not influence later work on this target.[8]

On 7 December 1941, the U.S. established censorship of international mail and communications. This should have given the Signal Intelligence Service all Russian traffic on the U.S.<—> Moscow lanes, as the cable companies were now required to turn over to the Censor a copy of every communication. The Venona traffic files contain Censorship copies of KGB traffic (N.Y.<—> Moscow) starting on 16 December. The early censorship coverage seems to have been quite complete, but then, unaccountably, the coverage drops off and from the end of Jan 1942 until mid-May, and for other short periods during 1942, significant gaps exist. In other words some hundreds of KGB and GRU messages from 1942 are missing and presumably were not taken from any source (that is, intercept and photography were cut back in favor of the seemingly more certain censorship source — so everyone dropped the coverage). The Army continued to intercept some Russian diplomatic on the non–U.S. lanes, such as Moscow <—> Tokyo. While 1942 KGB traffic is less likely to be readable than that of 1943 to 1945 (and GRU even less readable for 1942), the cryptanalytic success rate would presumably have increased had all the messages been available.[9]

By later 1942, censorship coverage had improved with nearly complete coverage on the U.S.<—> Moscow lanes. In summary then, on 1 Feb 1943, Miss Grabeel and Lt. Zubko had an extensive and ever-growing body of Russian traffic to work with, some dating back to 1939 (very little 1939 traffic has survived). Yet this certainly represented much less than half of what had been passed in those years.

C. Interlude: The Sinkov Mission to the UK

The United States entered into a de facto but limited Sigint arrangement with Britain in 1940, beginning with some discussions in London between the British Naval Intelligence Division and the U.S. Naval Attache. This came to nothing but in August 1940, a high level Army–Navy delegation went to the U.K. to evaluate British ability to continue the war. One of the American visitors, Brigadier General George V. Strong of the General Staff (and later Assistant Chief of Staff, G–2) told the British that the U.S. had solved the Japanese Purple (diplomatic) machine cipher. Strong then radioed General Marshall suggesting a formal exchange program for German, Japanese and Italian Sigint information. In Feb 1941, a U.S. mission went to GCHQ (sailing to England on the Royal Navy battleship George V which they had boarded at Annapolis). The party consisted of Captain Abraham Sinkov and 1/Lt Leo Rosen of the Signal Intelligence Service and Robert Weeks and Prescott Currier from the Navy's OP–20–G. The main purpose of the mission was to exchange information

[7]See "Catalog of Papers", Volume I, a collection prepared by AFSA in 1952 and held by the CCH. My summary of these negotiations is based on my notes from some earlier research.

[8]The Navy's lack of success on the Russian diplomatic target can be inferred from later Army—Navy discussions and the Navy's own summary of its work on Russian communications which reported no significant effort until the summer of 1943. Colonel Schukraft confirmed that the Army gave the Navy copies of all Russian intercept in the pre-war era , "because they were working on it. They told us they were."

[9]We surveyed the traffic logs and the boxes of actual traffic held in the Venona collection. Gloria Forbes, who joined SSA in 1943 and worked in the traffic section recalled that a significant gap existed in censorship coverage for 1942. (Interview by Benson and Phillips on 18 Dec 1991).

and material on the Axis powers (the British got Purple, the Americans learned a little about the Enigma break). The British gave Capt. Sinkov the following information about Russian systems:[10]

- Details of the Russian weather ciphers
- Information about OKK 5 and OKK 6, major Russian army and air force systems
- An NKVD air system
- Russian call-sign and radio procedure (army, air and NKVD/police)

In a hand-written note to his summary report on Russian systems, Sinkov concluded, "The Russian secret systems utilize a one part code book. These code books are super enciphered using additive, or special tables which vary from day to day."

Sinkov's report does not specifically mention Russian diplomatic or intelligence service systems or anything about the extent of British coverage of the Russian target. The British as we will see would soon make some important decisions about their coverage of Russian targets.

The British had obtained some Russian military codebooks and other cryptographic material from the Finns during the Winter War of 1939–1940 (the First Russo Finnish War) when Colonel John Tiltman, a senior GCHQ officer had visited the Finns to discuss Sigint collaboration. These codebooks represent a different trove than the so-called Petsamo material. The Petsamo cryptomaterial, which included a KGB codebook, instructions for using additive, tables and an emergency cipher system, came into Finnish hands in June 1941 at the start of the Second Russo Finnish War, reached the Swedes in 1944, and UK–US in 1945–46. We will discuss that in some detail later in this study.

D. The Decision to Begin the Russian Problem

Though putting two very junior analysts in a room on 1 Feb 1943 seems a small investment in resources, it represented a significant political decision considering the climate of the times and the considerable sympathy and admiration for wartime Russia held by many Americans. Unfortunately, we can find no date of decision and no policy papers that clearly relate to the decision. Frank Rowlett, one of the senior officers of the Signal Security Agency and later a senior official at NSA says that the decision to open the Russian problem was more or less inevitable considering the Army Sigint doctrine of the time.[11] That doctrine had come from Colonel Carter W. Clarke, Deputy Chief of the Military Intelligence Service (an operating agency of the G–2, Army General Staff) and head of the Special Branch. Clarke told Arlington Hall that in spite of the need to give maximum intelligence support to the war against Japan and Germany, Sigint collection against all other actual or potentially important targets must continue. That meant the Army was not to drop general diplomatic collection and should expand its cryptanalytic effort against those targets.

Clarke, a career Signal Corps officer who had been assigned to G–2 in 1941 (originally to head counterespionage) broadly controlled the Army's national Sigint programs and policies throughout the war and

[10]Sinkov report, undated but 1941, CCH Collection IV.v.7.5

[11]Rowlett interview by Benson, Orlando, Florida, 14 Jan 1992.

well into the Venona period[12] A sample of Clarke's thinking on Sigint policy can be found in his note of 6 May 1942 to Al McCormack, in which Clarke wrote of the need to present the most complete Sigint information possible to the national leadership about:

> *All those associated with and against us with the end purpose of enabling an American peace delegation to confront problems of the peace table with the fullest intimate knowledge possible it is possible to secure of the purposes and attitudes, overt and covert, of those who will sit opposite them.*[13]

The irony is that in terms of the Russian target, this worked the other way around. The Venona breakthrough didn't happen until after the "peace table" (Tehran, Yalta. Potsdam, San Francisco). The Russians came to the table with ample knowledge of our purposes and attitudes — through information provided to them by traitors whose deeds ultimately were revealed in Venona.

In June 1942, the Navy decided to drop its diplomatic Sigint program entirely and turn it all over to the Army (with the understanding that the Navy would still receive the product). The Navy reasoned that it had more than enough to do handling Japanese and German naval systems while "The Army has no (Japanese) military systems of immediate importance to occupy their efforts."[14] The Army accepted the offer and pretty much had to admit that at that moment it had very little Japanese or German traffic that could be exploited (German traffic couldn't be intercepted from the Second Signal Service Battalion's field sites; the Japanese traffic would soon be available in great volume, but the cryptanalytic problem was tremendous). This was one of those times when the Army wondered about the wisdom of covering or expanding coverage on diplomatic traffic of countries other than Japan and Germany. Perhaps all resources should be thrown against enemy military systems. We have seen Carter Clarke's position on this.

E. The Beginning of the Russian Problem at Arlington Hall

In early 1943, the Signal Security Agency had two major cryptanalytic and production elements. Section B II dealt with foreign code systems, including enciphered codes. Major Solomon Kullback, a pre-war civilian employee of the agency headed that effort. Section B III, under Major Frank Rowlett handled foreign cipher systems. This somewhat odd division of effort reflected the opportunities available to the agency and would soon be changed with the major breaks into Japanese army and Japanese military attache systems.

In the B II weekly report for the week ending 6 Feb 1943, Major Kullback included this short entry: "Russian: This section activated during the past week." In his report for the week ending 13 Feb 1943, Kullback had little more to say about the Russian problem except that some of the "Material edited and sent to the machine room." With that the trail grows cold and we see no more reports from the Russian unit for six months.[15]

---

[12]Clarke is one of the most important figures in the history of U.S. intelligence. He, more than any other individual, deserves credit for the post—war unification of Sigint. He arranged the Army's acquisition of Arlington Hall, Vint Hill Farms and Two Rock Ranch early in the war. He founded the SSO system and played a part in the creation of AFSA, NSA and CIA. He was, said Frank Rowlett, "a very unconventional man and he was also a man of considerable moral courage."

[13]From Volume I of the Papers of Colonel Alfred McCormack, in 3 volumes, NSA Archives, CBRF 42. McCormack, a law partner of John J. McCloy, had offered his services to the War Department after Pearl Harbor. McCloy and Secretary Stimson turned him loose on G–2 to examine the handling, analysis and dissemination of Sigint. The end result was Special Branch, headed by Carter Clarke with McCormack his deputy.

[14]John R. Redman, OP–20–G, to the Vice Chief of Naval Operations, 25 June 1942, subject: Cryptanalytical and Decryption Operations on Diplomatic Traffic. Author's collection.

[15]Weekly Reports of Section B II, NSA Archives, CBTB 34.

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

However, we do have one other significant report from that time, from a supporting organization, and some important anecdotal information.

In a memorandum of 15 Feb 1943, to Major Kullback, Mr. Sam Snyder, head of the Arlington Hall effort against the Japanese military attache systems reported:[16]

> *This week the work of identifying and compiling the Russian codes which have been transmitted in JMA was begun. At present the most recent of these Russian Codes is being compiled — a four-digit, two-part code called '024B' which was sent to Tokyo in November and December of 1942. As the messages in which these codes are transmitted are from blind stations and are sent at very high frequency, they are quite difficult to read because of the many garbles.*

Snyder based this report to Kullback on a preliminary study that had been completed several days earlier, to "record all quickly available information concerning Russian codes which have been transmitted in the Japanese Military Attache (JMA) system of enciphered codes".[17]

This research took place in direct support of the Russian problem just begun by Lt. Zubko and Miss Grabeel. If there was any single reason for the timing of the startup of the Russian problem, it probably came from information obtained from JMA, an enciphered code system that had been in use since Feb 1940 for communications between the Japanese Army General Staff and the Japanese military attaches. [18]

In a note for file on 21 Sep 1942, titled "Remarks on the Employment of the Russian Alphabet Supplement of the Japanese Military Attache Code", Snyder commented on some messages of 21 Oct of the previous year, Helsinki to Tokyo noting that when Russian values were applied to these messages, groups of Russian letters were obtained. Snyder concluded that "what we have here is the decoding part of a two-part Russian syllabic code in process of transmission to Tokyo."[19] The Japanese, it seemed, had acquired Russian crypto-material from the Finns.

The timing of the decision to start the Russian problem at Arlington Hall may have been partly inspired by a message from the General Staff in Tokyo to the attaches in Berlin and Helsinki: circular #906, 6 Oct 1942, to Colonel Hayashi and Major Horose[20]. The message was translated at Arlington Hall on 29 Jan 1943 (the Russian problem began on 1 Feb) and re-translated on 7 Feb. The Tokyo message begins:

> **We have commenced the study of Russian diplomatic and commercial codes and obtained the following results. For our information let us know how you are getting along.**

---

[16]CCH Collection, folder of weekly cryptanalytic logs, JMA 1942–43, IV.I.4.9a

[17]Unsigned "Memorandum on Russian Codes in the Japanese Military Attache System", with the hand written inscription "Feb. 9, 1943, First Report". In the NSA Archives at CBNI 17, see folders 9 and 10. This memorandum must have been prepared in part by someone familiar with Russian and other Slavic languages, as there is much discussion of not only the Russian alphabet but also "the usual Slavonic transliteration—cf. H—(Serbian X; Croatian H)". Snyder possibly knew some Russian. Zubko knew Russian and Ukrainian, while Ferdinand Coudert, who replaced Zubko, knew Russian, Serbo–Croatian and Bulgarian. Another possibility is that Meredith K. Gardner, then working German Dip, wrote the memo. Gardner had privately studied Russian in 1937. He told me in 1993 that he defintely worked on JMA messages carrying Russian crypto intelligence following his assignment to the JMA unit in mid-June 1943.

[18]See "A Brief Sketch of BI–M, n.d.(but 1945), in Box 2 of the Sam Snyder Papers, CCH Collection, XI.K.2. JMA was subdivided into JAS and JAS–1, the basic JMA systems and JAT which would later be used by the attaches (actually the Sigint reps in the office of the attache) for exchange of information on the solution of foreign cipher systems. Crypt intelligence appears at one time or another in all the JMA systems.

[19]"SSS Diary", Box 2 of Snyder Papers, CCH Collection XI.K.2

[20]See folder marked "Jap Dip Dispatches", in the Venona Collection, Provisional Box 1.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

The Japanese General Staff reported their findings on at least five separate Russian systems, giving short paragraphs on each and accounting for all the systems that the U.S. would later include in Venona. The Japanese had not solved any of the Russian diplomatic, but they had made some progress, providing enough clues to inspire an effort at Arlington Hall.

The most important information passed by Tokyo concerned the Russian Trade system (known as [redacted] in Venona). Tokyo reported that the indicators appeared in the first group of Trade message texts: "the first and second digits of the first group of the text gives the length of the message — the fourth and fifth digits give the additive page." Other important JMA messages available to Zubko and Grabeel, during Feb 1943, included:[21]

• Berlin to Tokyo, 15 June 1942, 87401–02. JMA Berlin reports that he had just received the five figure 023–A code, "which the German army recently captured from the Russians."[22]

• Berlin to Tokyo, #89200, 17 June 1942 (translated at Arlington Hall 16 Dec 1942). The attache in Berlin reports on two Russian military systems, the aforementioned 011–A, described as a high command system and 023–A, a general military system.

• Helsinki to Tokyo, #957, 19 Oct 1942 (translated 30 Dec 1942). The attache in Helsinki asks Tokyo to send him a "reference collection" regarding Russian military communications, "since Japan has had success in deciphering these messages." He also reports that Finland had stopped studying one of the major Russian (military?) systems because, "they did not have telegrams using identical additive."

• Berlin to Tokyo, #405, 21 Oct 1942 (translated 7 Jan 1943). Discussion of the possibility that the Russian high command was using a machine cipher.

• Helsinki to Tokyo (and to other attaches), #032, 11 Jan 1943 (translated 25 Jan 1943). The attache transmitted various Russian military code values and reported that the Finns had recovered about 1000 values. He also gave information on the Russian Arctic naval code. He concluded that , "It is reported that the British are directing the Russian codes." (the meaning of this latter item unknown, rlb).

More would be available from JMA (and its sub-system JAT) over the next two years, and we will return to the topic shortly.

Lt. Zubko and Gene Grabeel, therefore, had quite a bit of material to work: back traffic, current traffic, analytic assistance from Sam Snyder's unit, and the resulting texts from JMA messages that guided their analysis —particularly the understanding of cryptographic indicators. Zubko recognized that the diplomatic traffic could be divided into two major groups based on external address: Trade messages which bore the message address of the Ministry of Trade, and diplomatic messages with the Foreign Ministry address. Trade accounted for almost 75% of the traffic. Zubko also discovered (presumably guided by the JMA messages) information about the indicator group: .

[21] I have used the messages quoted in in the 9 Feb 1943 memorandum (no signature), and the messages in the "Jap Dip Dispatches" folder, previously cited, to reconstruct what was available to Zubko and Grabeel.

[22] In this message JMA Berlin also reported that,

> **Germany is anxious to get hold of code messages sent by the American Military Attache in Cairo and Kuibyshev (the Moscow evacuation point) to Washington in order to ascertain the condition of the British and Russian Armies. As this is most important material the Germans would like to get hold of it, if you can intercept American Attache telegrams from these two places and a number of other places as well, please let us know.**

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

> *He observed that the last two digits (01 to 50) operated like a page and that the third digit (1 to 7) gave the number of pages with 60 groups to a page) used in the particular message. He also noted that some relationship existed between the indicator group and the third group of the message.*[23]

However, neither the Japanese nor Zubko correctly identified the first two digits of the indicator group.

F. The Russian Problem Put on Ice[24]

The Russian problem had run for two months (and probably less than that) when it was mysteriously suspended. Unfortunately, the mystery remains.

One morning (March 1943) when Gene Grabeel reported to work, she was told — but she does not recall by whom — that the program had been dissolved, and that she should report to Major William F. Edgerton for a new assignment. She had no advance notice and never learned why this happened.[25]

According to Cecil Phillips, Major Bill Smith, a later head of the Russian problem, told him in 1944 or 1945, that the project had been shut down because Lt. Zubko had become too friendly with Major Geoffrey Stevens, the British liaison officer at Arlington Hall.[26] The U.S. did not share with the British the fact of the effort against Russian diplomatic communications, a policy which continued for another two, and close to three, years.[27]

Stevens and Zubko had probably met in later 1942 when Zubko, newly arrived at Arlington Hall, had been working the Japanese military attache problem (during his short tour at Arlington Hall, Zubko worked in both B II and B III). Stevens took particular interest in JMA, as it was also being worked by the British. Much JMA material was being exchanged between the US and UK, and one can imagine some discussion between Zubko and Stevens about the JMA messages that contained information on the cryptanalysis of Russian systems. But for some strange reason, surely by accident, the two-person Russian problem had been placed in the very office (a private office, not a bay) whose only other occupant was Geoffrey Stevens, who was not supposed to know what Zubko and Grabeel were doing! Gene Grabeel recalled how, given the security admonition from Frank Rowlett, she and Zubko spoke only in whispers, and she never had a real conversation with him. She saw Zubko once shortly after the program stopped, but Major Edgerton seemed to intervene, discouraging any conversation. She never saw him again.

Mr. Zubko gave me some information in a brief telephone conversation (made in an effort to set up an appointment). He said that he did not recall the names of anyone at Arlington Hall except Major Stevens, whom he had found to be a kindred spirit (both had trained as infantry officers). He did not enjoy the work at Arlington Hall and believed he wasn't suited for it. As for the abrupt closedown of the problem, he said that he was reassigned out of Arlington Hall in a great hurry, but he never knew why. He told me that he had been in contact with the Russians in Washington, in an official capacity, as "they were our allies." Mr. Zubko's later military

[23]1/Lt Richard T. Hallock, "ZYT Report—6/8/44", Venona Collection , Provisional Box #1.

[24]Put on Ice—a favorite KGB tradecraft term in the Venona messages, meaning that an operation would be suspended or an agent deactivated until the operational security climate improved.

[25]Grabeel interviews.

[26]Stevens had been with the GCHQ unit in Singapore and had been evacuated after the Japanese invasion. Frank Lewis, an Arlington Hall veteran who made important contributions to the fundamental break into Russian Diplomatic, recalled Stevens as "brilliant". Meredith K. Gardner had worked JMA with both Zubko and Stevens, but he could shed no light on Zubko's departure.

[27]Frank Rowlett, Ferdinand Coudert and Oliver Kirby told me that the Russian problem was U.S. eyes only during 1943–45. SSA records include some contemporary references to this policy (discussed later in this study).

service included behind the lines activity in China. Mr. Zubko declined to be interviewed or to correspond on his service at Arlington Hall, citing the fact it was so long ago and he could not remember much about it.

During the research for this study we asked many interviewees if they recalled anything about the suspension of the Russian problem. After much effort, we found nothing, but at least we found that the mystery was long standing. In March 1946 Colonel M.A. Solomon, G–2, inquired about the origin and history of the Russian problem. The answer, from Lt Col James B. Greene of ASA suggests that the early history of the program was already clouded. Greene wrote that, "for reasons not known to personnel now at ASA, the Russian problem was first begun in late 1942, (employing two persons), was for some reason abandoned soon after, and was again started in the Spring of 1943." As we have shown, the project started in Feb 1943, not late 1942. A curious element of Greene's reply to G–2 is that it was drafted by Bill Smith, who perhaps wasn't anxious for the General Staff to know too much about this matter.[28]

In a paper written in 1965, "Recollections of Work on Russian" , Frank Rowlett commented that "the first Russian section was short-lived, for some reason which I do not remember it was disbanded."[29]

G. The Russian Program Resumed

As with the original short-lived program, we lack documentary material to account for the decision to re-open the Russian problem. But we do have the recollections of those who were there — once more Gene Grabeel, now joined by Ferdinand W. Coudert.

Captain Ferdinand Coudert, early head of the Russian program at Arlington Hall.

Coudert had been directly commissioned into the Signal Corps as a 1/Lt and was ordered to active duty on 24 Oct 1942. His background — should the material prove to be exploitable —was especially suitable for the Russian problem. A member of a famous international family law firm, Coudert Freres, he had BA and MA

[28]The Greene memorandum dated 12 March 1946, subject: History of Bourbon Problem" is in the NSA Archives, CBNI 21. Col Greene would have been correct in giving the date of 1942 if he had reference to the Russian weather material, briefly worked at Arlington Hall in 1942 and then turned over to the Navy.

[29]This paper, 6 pages with enclosures, is dated 11 Feb 1965. Located in CCH Collection, VII.83. During my interview with Mr Rowlett, he could recall nothing about the shutdown of the Russian problem.

degrees from Harvard, the latter in Slavic Studies, and a law degree from Columbia. He knew French, German, Russian, Serbo–Croatian, Bulgarian and had completed two crash courses in Japanese at Columbia.[30]

His early military assignments or misassignments included supply and motor maintenance courses at Fort Monmouth. He escaped from these in late November 1942 for duty at Arlington Hall, where he first worked as night security duty officer and courier. He briefly worked on the Japanese Army problem but failed an ad hoc oral language test by Colonel Doud (head of B Division, the Sigint production organization) and transferred to the German problem. One day in April 1943, Major Kullback, head of section B II called him aside for a conference in a vacant office. Kullback told Coudert that the agency intended to begin working Russian diplomatic, and that he would run the effort. Kullback did not tell him about Lt. Zubko's earlier effort. Kullback emphasized that the program was ultra secret and was not to be discussed within the agency. It would not be shared with the British — Coudert recalled that this seemed a touchy matter.

Gene Grabeel recalled that the program re-opened in about April 1943. A senior officer at the Hall, perhaps Major Edgerton, took her to meet Coudert and asked her to introduce him to the Russian problem. She and Coudert worked in two offices during their time together, at first in a room with two long tables separated from other work areas by filing cabinets. They resumed sorting the back traffic and the new material which was delivered about once a week. Just as when she had worked with Zubko, this remained a compartmented activity — she and Coudert whispered to each other or worked in silence. Colonel Doud and Major Kullback visited a couple times, but otherwise they worked alone for about two months.

The operation slowly built up with the arrival of the following people:

Josephine Miller, late May
Carrie Berry, mid-July
Mary Boake, mid-July
Helen Bradley, August
Gloria Forbes, September

Their backgrounds, similar to Miss Gene Grabeel's, are representative of the recruiting and hiring strategy of Arlington Hall during 1943. Miller, Berry, and Boake had been schoolteachers (Miss Boake with a recent Master's from the University of Oklahoma). Boake and Berry were recruited by a letter offer from the Signal Corps. Miss Berry recalled that the offer, at the grade of SP–5, paid $1800, plus a bonus for Saturday work, double her salary as a high school teacher in Dawson, Texas. Gloria Forbes came to Arlington Hall following graduation from the Mississippi College for Women. During her senior year she took a correspondence course in cryptanalysis. The War Department sent her the course materials, and she mailed her assignments to

[30]Interview of Mr Coudert in Key West by RL Benson, 15 Jan 1992. Mr. Coudert's father, Frederic, represented the French, British and Russian (Czarist) governments before and during the First World War, and he represented the democratic provisional government of Kerensky before the Communists seized power in Russia. The senior Coudert was a neighbor and good friend of Theodore Roosevelt. Mr. Coudert's brother, Frederic Rene Coudert (1898–1972) was a member of Congress from 1947 to 1958, representing the Silk Stocking district of Manhattan. Ironically, Congressman Coudert, while a member of the New York State Senate had co-chaired the Rapp–Coudert committee before the war, looking into Communist activities in the New York school system. The associate counsel for the Rapp–Coudert committee, Philip W. Haberman Jr., later joined (or at least was recruited for) the Special Branch of G–2, the organization that controlled the Arlington Hall product. Al McCormack of Special Branch noted that "Haberman keeps the committee files in his law office, and they are one of the most fertile sources of information on Communists and activities in and around New York — the G–2 people at Governor's Island have got acquainted with him." (see Personal Papers of Colonel Alfred McCormack, page 38, NSA Archives, CBFH41). The U.S. part of the Venona story is significantly concerned with KGB agents connected to the Communist Party in New York.

Washington. She never found out why the Army contacted her or got her name (Miss Boake had also been offered this course but had declined).[31]

The unit then moved to a private office, for better compartmentation, but would again move to an open bay, once more defined and screened by rows of safes and cabinets.

We have no record of the earliest cryptanalytic attack on the Russian Dip systems by Coudert's unit. Russian military traffic, in low grade crypt systems, became available from Army and Navy intercept in mid-1943, and the JMA systems continued to provide information relevant to all types of Russian traffic.

G.1. More About Recruiting People for Arlington Hall

This subject seems interesting and important enough to say a little more. We have seen that Lt. Paavo Carlson recruited Miss Grabeel in Lynchburg, Virginia. Carlson's own experience is instructive in the (effective) ways of the military in an emergency.[32]

Carlson, an infantry officer, was ordered to Arlington Hall from First Army, Governor's Island. As with Lt. Zubko he didn't know anything about the place. He reported for duty on the Monday before Thanksgiving, 1942, and took care of administrative matters that day. On Tuesday he found that he had been detached from Operations (of which organization he knew nothing as yet), on Wednesday he was briefed on recruiting procedures and on Thanksgiving morning he was in Lynchburg looking for civilian recruits.

Arlington Hall before the war. This postcard was used by Army recruiters.

[31]Interview of Forbes and Boake by Benson and Phillips, 18 December 1991 in Reston, Virginia. Cecil Phillips telephoned Berry and Miller in early 1992. The Signal Security underwent tremendous growth during 1943, hiring 4067 civilian employees that year (compared to only 741 during the first year of the war), including 684 in January (the largest monthly total of the war). Space had become available with the purchase of Arlington Hall and Vint Hill Farms and the demand for people was especially driven by the breakthroughs into Japanese Army systems, notably the famous Water Transport code which was entered in early 1943. (See History of SSA, Volume One, Part II in CCH Collection, IV.B.1.1)

[32]Interview of Paavo Carlson by Benson and Phillips on 24 August 1992.

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

He was one of six lieutenants dispatched from Arlington Hall in late 1942 looking for college graduates to bring into the Signal Security Agency as quickly as possible.[33] Carlson remained in the field into May 1943 working out of the post office in Lynchburg and later the John Marshall Hotel in Richmond. As he knew nothing about the work of Arlington Hall, he had no difficulty with a cover story — he could only tell recruits that their employment would involve secret work near Washington, D.C. He had little contact with Arlington Hall during this period, returning there just once to file travel vouchers (which he learned about incidentally — he had assumed that he had to pay for his operation out of his own funds).

These six officers seem to have recruited the majority of the degreed people hired by Arlington Hall in 1943, and some 90% were women.[34]

H. Russian Military Traffic 1943–44

The early efforts against Russian military communications have no direct bearing on the Russian diplomatic problem. But the intercepted material did give Coudert's people some cryptanalytic experience —in fact the first decryption success against the Russian target. For Coudert himself, and Commander Taecker, his counterpart in OP–20–G, the Navy Sigint organization, it finally gave the opportunity to use the Russian language. And it inspired the first training programs on the Russian target — elementary Russian language training, Russian geography, politics and history — taught by Coudert. In any case, the chronology, if only in outline, of the beginning of the various phases of the U.S. effort against Russian targets seems important to record (the same for the UK experience).

The Army began casual intercept of Russian military traffic during 1942 (we know that weather traffic had been copied during that year and Arlington Hall briefly worked the simple crypt systems, turning the project over to the Navy in December). In January 1943, Arlington Hall published a short circular which discussed the characteristics by which Russian Army, Air Force and weather traffic could be recognized. The study included a short description of some Russian crypto procedures, call-sign procedures, net structure, and drew attention to the poor calibration of Russian field radio sets. The circular emphasized recognition of traffic rather than systematic collection.[35]

We have specific information on the beginning of the Navy's intercept of Russian military communications, as well as their cryptanalytic efforts, and of particular interest, the cooperative work of the Army and Navy.

On 6 July 1943, Lt. Cmdr. C.H. Taecker (USN ret.), a Slavic linguist and scholar, and former attache, began a study of Russian cryptographic systems, at OP–20–G, the Navy's Sigint organization. On 14 July, the Navy began regular interception of Russian traffic at Station S, Bainbridge Island, Washington using a four shift single

[33]In Lynchburg, Carlson replaced a retired Army officer, a Captain Hoffman who had been there for a short time on behalf of Arlington Hall. Hoffman, who wore a World War I campaign hat, had Carlson sit with him and a Civil Service representative for a day— then he departed.

[34]Carlson recalled that one of the lieutenant recruiters had oversold Arlington Hall in making his recruiting pitch: he showed some of the young women photographs and postcards of Arlington Hall when it had been girls school and had a riding stable and swimming pool. When these new hires arrived at the Hall they found a somewhat changed atmosphere, and the lieutenant was anxious not to come face to face with some of them.

[35]Circular, "Intercept Information, Russian Radio Operations (SIGLWO)", 26 Jan 1943. A covering letter is signed by Major Harold McD. Brown, of SSA. NSA Archives, CBTE 41. The SSA's Second Signal Service Battalion site in Alaska probably intercepted the Russian military traffic. Virtually all Russian military,naval, air, weather and police/NKVD traffic was taken from Far Eastern nets (essentially Siberia).

position watch.[36] Shortly before that, Lt Louis Tordella, OIC of Station S had received a dispatch from Captain Wenger of OP–20–G directing him to set up an isolated room staffed by his most competent operators and begin intercepting the communications of Russian naval forces in the Far East.[37] Tordella received [redacted] dated 1938 or 1939 that had been obtained from the British — probably during the Sinkov/Currier mission to Bletchley in 1941.

Tordella and his operations chief, Orville Coonce, selected the following experienced intercept operators to begin copying and studying Russian naval traffic: Harvey J. Howard, Hubert A. Price, Charles Quinn, Rodney Whitten and (fnu) Gwindon. Tordella, Coonce and the operators performed rudimentary traffic analysis. He gave this target highest priority, except when there was an emergency need for total resources on Japanese naval nets using JN–25.[38] The intercept usually went airmail to Washington, but Dr. Tordella could not recall any discussions with analysts working Russian naval back at Nebraska Avenue.[39] It was Dr. Tordella's recollection that Station S strictly took Russian naval traffic.[40]

In August the Army and Navy began to exchange traffic and Commander Taecker received three enlisted people and one civilian to work on the Russian project. This compares favorably to Lt. Coudert's resources at the time (however, Commander Taecker's unit also had a Russian typewriter!) According to an informal Navy account of those times, "it was decided by higher authorities that the Army and Navy would have joint but not combined liaison on the Russian project."[41]

By that time (and certainly by the end of the year) the Army and Navy had adopted the covername "Blue" for the Russian problem.[42] The Navy seems to have used the term "The Blue Caesar" for an ongoing series of reports on Russian radio nets and the crypt systems seen on them. Each net was named for a Roman emperor (the Nero net, the Caligula net etc.)[43] In April 1944, four additional intercept operators joined the Russian

---

[36]"Russian Language Section History, 1943–1948", an undated, informal survey of, despite the title, intercept, cryptanalysis and production. NSA Archives, AHA 202. Mr. Coudert and Cecil Phillips, who collaborated with Commander Taecker, provided background information about him. They especially recalled his courtly, aristocratic manners.

[37]Discussions with Dr. Tordella, 3 December 1992, Benson and Phillips. We talked about the beginning of the Russian problem and some later political and resource aspects of Venona.

[38]The Russian naval position got first place in the competition for voltage among the various target positions at Station S.

[39]Dr. Tordella thought Ham Wright might have been overseeing the Russian naval problem at OP–20–G. He did not know Commander Taecker and until our discussion had not been aware of the latter's unit.

[40]This is of interest because Cecil recalled that in 1944, both Coudert and Taecker were working NKVD military/police ciphers — however, this included the NKVD (KGB) "naval", that is coastal patrol, traffic.

[41]Ibid. Unfortunately, I find no other record of the decision or the identity of the "higher authorities". Nonetheless, the fact of the liaison is well-remembered by Mr. Coudert and Mr. Phillips, and some examples of the joint effort amply documented.

[42]Sensitive projects were color-coded e.g., the "Silver" traffic was a second in that series (and there were at least one more). However, color coding had also been used on some of the main targets, such as Orange for the overall Japanese target (Orange designated Japan in Army and Navy war plans) and later Yellow for some aspects of the German problem. Oliver Kirby described these special projects as "encapsulated programs, some of them experimental or of short duration and very sensitive."

[43]Mr Lou Maddison, GCHQ veteran and Sigint archivist, told me that the Navy's Blue Caesar program began in the summer of 1943 (discussions at GCHQ, Maddison and Benson, 6 May 1992). Our Blue Caesar papers bear no signature or agency heading, and the attribution to the U.S. Navy is based solely on Lou Maddison's information.

operation at Bainbridge and in June four operators began a watch at Station W, Winter Harbor, Maine.[44] During 1943–1944, the units headed by Lt. Coudert and Commander Taecker cooperatively worked a number of military and police systems, Lt (j.g.) Moeschl of OP–20–G working within the Russian section at Arlington Hall and Coudert and Taecker meeting weekly. Some of the Russian systems they studied included:

B–20 and B–21. Ship and air movements. Broken in 1944

B–28. Radio service messages. Simple substitution.

B–40 (ZMQ). Intercepted from July 1943. Radio service messages, postal reports in 3 digit, simple substitution.

B–43 (ZMO). Recognized in Sep 1943. Minor military administrative matters. Readable.

B–44 (ZMP/ZYP). Intercepted from Sep 1943. Minor military administrative matters and Communist Party instructions. Readable.

Much of this material was extremely simple cryptographically and rarely contained anything of interest, while other systems that might have been of interest could not be copied. Lt. Coudert recalled a Russian police or military message dealing with good places to go fishing — he said that this was a typical message. We read a comment (probably by Coudert or Taecker) about B–43/ZMO traffic, that "some of the material mentioned is rather unbelievable, and it is just possible that when an item such as 'red bilberry' [a shrub, RLB] is mentioned, it might have an entirely different meaning to the recipient of the message"; in other words, an open code underlying the plain text. Other messages concerned production of vegetable crops, care of animals and repair of railroad cars. But it was a start on Russian systems. We should mention that the Navy credits their Mrs. Leora Cunningham with "the first break into Russian cryptographic systems, by either Army or Navy" in Oct 1943, by her study of "traffic being received from both the Army and Navy".[45]

I. More Japanese Military Attache Messages

In August 1943, Sam Snyder, head of the Japanese Military Attache (JMA) problem at Arlington Hall, renewed his support to the Russian problem. Some of the entries in Snyder's diaries for 1943 include:[46]

- 2 August. Conference with Captain Marston re liaison with Lt. Coudert.
- 3 August. Completed compilation of messages re Russian system.
- 4 August. Spent rest of afternoon working with Mr Millard (from the Language Branch) on message re Russian Diplomatic Codes.

[44]"Russian Language Section History". Dr. Tordella recalled that in early 1945, the Skaggs Island Station, which he commanded after having been OIC at Station S, began a search for a "two channel TTY multiplex, 110–140 repitition rate" on orders from Washinton. They found the signal, developed equipment to process the traffic and reported their success to OP–20–G. He then learned that the Army SSA station at Two Rock Ranch had also begun to take Russian printer traffic (Spike Neal headed this Army program). However, in the earlier period, 1943–44, Tordella had no contact with the Army concerning intercept of Russian manual morse (which was what Station S was doing). (Benson/Phillips discussions with Dr. Tordella, 3 Dec 92)

[45]Ibid. See also these important sources: "The Blue Caesar", Report # 18 (summary up to 18 Sep 1945) in the NSA Archives, CBPI 46 and reports on each Russian military crypt system for 1943–45 in the folder "Russian Codes and Ciphers" in the NSA Archives, G030104–4. Also "The Blue Problem", a supplement to the Annual Report of B Branch, Signal Security Agency, 1 July 1943 to 30 June 1944, CCH Collection IV.c.5.6. We don't know what break Mrs. Cunningham made, but it was not in Russian diplomatic. As we'll discuss, there are several claimants at Arlington Hall for the first fundamental cryptanalytic discoveries, during 1943, about Russian diplomatic systems. The first complete decrypts of low-level Russian military messages probably date to the end of 1943 or Jan 1944. The first reading of diplomatic (Trade only) began in later 1944, but in small fragments only (such as the identification of the codegroups used to give numbers).

[46]In CCH Collection, XI.K.2. Box 2 of the Snyder Papers, Snyder diary for 2 August 1943 to 30 June 1944.

Frank Millard. He played a role in examining JMA for references to Russian cryptography.

- 6 and 9 August. More discussions with Millard.
- 11 August. Visited Lt. Coudert re Russian message.
- 13 August. Helped Millard complete messages re Russian Diplomatic Codes. Gave material to Lt. Coudert.[47]
- 19 Oct. Visited Frank Lewis who is doing a special problem for Lt. Coudert.
- 24 Nov. Major Rowlett and Captain Smith visited to see (Lt.) Mikofsky's work on Russian — arrange closer coordination both ways.

The JMA message that probably caused the excitement during August was a circular, Tokyo —> JMA Helsinki and Budapest, D 1835, sent 6 April 1943 (but not available until July or August). That message began: "We have begun to read the Russian Foreign Diplomatic Code used for communication between the Consuls in Seoul and Dairen in communication with Moscow and Vladivostok." The message contained a wealth of cryptanalytic information including the statement (after a description of the relationship of opening code groups in Russian messages) that "This gives you the starting point in the additive table, and from this as a starting point, the additives are used consecutively."

Other relevant JMA messages that Snyder would have made available to Coudert included:

- Tokyo to JMA Berlin, 29 Jan 1943 (translated 18 March 1943) refers to a 5-digit Russian code and the possibility of a Russian machine system.
- JMA Berlin to Tokyo, 6 Sep 1941 (translated 15 April 1943) in which the attache reports that "Today we received the Russian military code OCKK 7" and that the code values would be radioed to Tokyo.

The latter and other JMA messages mention the Russian crypto-material recovered at Petsamo, such as "a diplomatic code which was being burned by the Russian Consul in Petsamo was captured and reconstructed."

[47] 1/Lt J. Leslie Hotson prepared a report dated 22 August 1943, "Report on Progress of Work on Russian Codes Sent in Japanese Military Attache System", which, he noted, supplemented the 8 February 1943 Memorandum, "and should be used in connection with it." Most of Lt. Hotson's report concerns Russian military systems. On file in NSA Archives at CBNI 17.

This was KOD 26, a system used between the Foreign Ministry and the consulates and which would later be available to the US–UK for Venona purposes.

JMA, and its special crypt-intelligence subseries, JAT, continued to give clues to Russian systems for the rest of the war. Once JAT was fully solved, in about Nov 1944, a tremendous amount of material became available. It had become apparent well before then that Japanese military intelligence had Sigint liaison officers in the Axis capitols, Berlin, Budapest and Helsinki, who received and provided cryptologic materials on many allied and neutral targets including the U.S. and Russia. It had also become apparent that the Finns especially had seized important Russian diplomatic and military materials, the diplomatic at the Russian consulate in Petsamo, Finland on or about 22 June 1941 (the date Germany invaded Russia) when Germany and Finland became de facto allies. Shortly before Finland obtained an armistice with Russia in 1944, the Finnish Sigint organization and the JMA evacuated to Stockholm. But the Finns continued to cooperate with the Japanese Military Attache who also withdrew to Sweden.[48]

In a message of 18 Jan 1943 (not translated at Arlington Hall until 4 July 1945) the JMA Helsinki wired the Vice Chief of the General Staff with some concerns about the security of the JMA crypto-systems. He noted that, "Recently all countries have been devoting great energy to cryptanalysis, and they have made remarkable progress. For instance, Finland has decrypted Russian, American and Turkish codes" and "in view of these facts it seems necessary to take the utmost precautions to secure the security of our present codes." He warns Tokyo about the vulnerability of the JMA system, especially the re-use of additive key. But in conclusion he said, "I suppose that it is hazardous to instruct the higher authorities (therefore) I will cut this short."

J. Progress on Russian Dip

On 1 Sep 1943, Arlington Hall re-organized in a fundamentally important way. Section B II (Lt Col Solomon Kullback) was now to work solely on the Japanese Army target. Section B III (Major Rowlett) assumed cryptanalytic and reporting responsibility for everything else, including the Russian problem, which became known as the Special Problems Unit, designator B III b 9, Lt Coudert remaining in charge.[49]

The Russian diplomatic problem now began to receive more attention and resources. Just at about that time Arlington Hall completed a Morale Survey of each element of the agency. The report of that survey includes a short entry on Lt. Coudert's operation, giving us the names of the people then working the Russian problem and an evaluation of the operation. The people in the unit were divided into several informal units:

Lt. Coudert, OIC
Helen J. Bradley, technical advisor

Gene Grabeel
Doris Johnson
Ruby Roland

[48]The Finnish army did not cross into Russia immediately on 22 June 1941, although they had established a secret alliance with Germany by that time. A few days later the Russians pre-emptively bombed Finnish positions and the Second Russo —Finnish War began. However, the KGB and GRU and the consular people probably evacuated their Petsamo station on 22 June , but failed to destroy everything. Petsamo became Soviet territory at the end of the war. See the study, "JAT — The Solution of the Japanese Military Attache system for Crypto-Intelligence", issued by ASA 31 July 1947, NSA Archives, CBMJ 57.

[49]This reorganization was made in recognition of several major breakthroughs in 1943, especially into high grade Japanese Army systems. The tremendous volume of material, of very high intelligence value, required a maximum dedicated effort. Likewise the JMA and Purple had become a major source of information on strategic developments in Europe. JMA, all Dip and everything else that was not Japanese Army went to Rowlett.

Carrie B. Berry
Mary L. Boake
Juanita McCutcheon
Rosa Brown
Josephine E. Miller

(b) (1)
(b) (3)-18 USC 798
(b) (3)-P.L. 86-36

The narrative statement of work reports that the unit was receiving an average of 2500 messages per week, and the number was increasing, especially the Trade and Diplomatic. In addition to the permanent party, three clerks were loaned in to help with the logging. Further:

> *The efficiency of the unit is good. There is no idleness and few complaints or grievances arise. Thus far, the work has been negative in results. The aim is to break the systems and a staff of experts would be of value to the unit.*[50]

Indeed, the need for a "staff of experts" and a professional cryptanalytic effort was now becoming apparent, but processing the ever-increasing amount of traffic and concerns about compartmentation continued to occupy Lt. Coudert. On 3 Sep 1943 he reported to Major Rowlett that along with Russian diplomatic, including Trade, and Russian plaintext, miscellaneous traffic such as [redacted] Greek diplomatic (governments in exile) was being routed to his section, "to prevent the traffic section from learning that we were dealing with a Russian problem." The Russian traffic was being sorted according to system and lane and (external) message number; the indicators determined and handwritten on the face of each message along with the group count.[51] A week later Coudert reported that his unit had received 4000 messages during the past week, 865 Trade, 300 diplomatic, 800 plaintext "and the rest not yet characterized."[52]

The minutes of the B III Executive Council (which at various times during 1943–45 was called the Cryptanalytic Research Committee or Group, and finally the Intelligence Division Executive Council) give us some sense of the progress of the Russian problem during later 1943 as discussed by Frank Rowlett and his principal assistants:[53]

- 2 Sep. More experienced cryptanalysts needed for the Russian problem.
- 4 Sep. Lt. Coudert to give a status report with recommendations.
- 7 Sep. "It was pointed out that with regard to the Russian problem the British know nothing about it."
- 9 Sep. Both Russian military and diplomatic to be exploited as much as possible.
- 11 Sep. IBM processing of Russian traffic would be handled in a special category.
- 14 Sep. The Navy to be given duplicate copies of Russian traffic.
- 16 Sep. Major Rowlett noted Lt. Coudert's recommendations: experienced cryptanalytic people would be of value to the problem; training needed to be expanded.

---

[50]"SSA Morale Survey 15 July–1 August 1943". NSA Archives CBTD 31 in folder marked "Signal Security Agency". The newest employee of the unit, "Miss Johnson, recently of North Carolina" was interviewed and provided some nice personal experience information. Miss Johnson, of course, was a schoolteacher (or at least had a recent degree in education). The survey report gives a candid view of wartime civilian employment in Washington.

[51]Coudert memo for OIC, B III, 3 Sep 1943. CCH Collection, IV.c.7.4 in a folder marked "Processing of Traffic 1943". The internal serial number, that is the one-up number of the true sender (KGB, GRU etc.) was encrypted in the text, and at that stage, unrecovered.

[53]In B III b weekly report signed by Captain E.J. Wrigley. NSA Archives, CBTB 34, in folder marked "SSA Weekly Reports Jan to Oct 1943."

[53]See folder marked Intelligence Division Executive Council, 1943–1946 in CCH Collection IV.c.6.2.

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

• 30 Sep. Colonel Cook (head of B Branch) rejected the notion that Russian Trade material should be sent to the Bureau of Economic Warfare (note by RLB: The KGB had, as Venona would later show, significantly infiltrated the BEW).

• 13 Nov. Rowlett reported that "definite leads" had now been developed regarding the Russian traffic and that "Mr. Lewis and Lt. Elmquist should be commended for their work in this connection." However, because of the urgent demands of the Japanese problem, they would have to be relieved of from their work on the Russian program.[54]

These "definite leads" included the discovery that the Russian Trade traffic (then called ZYT by Arlington Hall) was an additive system, that is, an additively enciphered code. The Russians were using a code book of unknown size (that is, the total number of values unknown), and to each code group or value selected from the book to create the message, applying an additive to create a cipher group — the group that would be transmitted in the message. The problem then would be to "solve" the additive, and strip it off to reveal the true code group, and then obtain the individual code group values (their meaning) by book-breaking. The latter would be accomplished by tedious analysis or by somehow acquiring the right code book. The biggest problem would be to solve the additive (also called the cipher or the key). If it was from a true one-time pad it could not be solved.

Lt. Coudert's people were re-enforced during Sep–Oct 1943 by, at least, Lt. Richard T. Hallock, Mr. Burton Phillips, Lt. Karl Elmquist and Mr. Frank Lewis (Mrs. Genevieve Feinstein and Miss Mary Jo Dunning; and Cecil Phillips would come onto the problem during 1944). They were all experienced cryptanalysts —and several had strong academic backgrounds. Lt. Richard Treadwell Hallock had received a Ph. D. from the University of Chicago in 1934, in ancient Near Eastern languages. He subsequently joined the faculty of that school's Oriental Institute. During his long academic career he published many works on ancient cuneiform writing (Assyrian).

By the time these people arrived to help, Coudert's unit had been able to divide the Russian (non-military) traffic into a number of systems which he called [redacted] and [redacted] and [redacted] and [redacted] the latter two being Trade and the [redacted] systems passing as Diplomatic. Beginning in July and into December 1943, Mary Boake studied system [redacted] issuing five research reports during November and December. She reported that [redacted] (soon re-named ZZB) appeared on 24 traffic lanes but only Washington <—> Moscow carried enough traffic to work with. She concluded that none of her studies showed any particular results and the work was discontinued for some 6 months.[55] [redacted] would later be designated as [redacted] the system for Russian Naval Intelligence (GRU–Naval). Carrie Berry and Miss McClelland studied system [redacted] (later ZZC/ZZD, and still later known as [redacted]) during this same period. As with [redacted] machine runs were made with no useful results. Traffic on the Los Angeles, New York, Washington, San Francisco lanes (to and from Moscow) and the New York <—> Ottawa lanes was studied.[56] System [redacted] would later be identified as GRU.

[54]Captain Bill Smith later told Cecil Phillips that there had been some rivalry between Rowlett and Kullback on this point. Apparently some of those detailed from B II to B III to help on the Russian problem told Kullback about the breakthrough without informing Rowlett first.

[55]Informal reports on DB: 10,18,25 Nov 1943; 1 and 8 Dec 1943. Venona collection, Provisional Box #1. Mrs Hare and Mrs Hill assisted Miss Boake in these studies.

[56]Informal reports on DC: 18 Nov and 2 and 9 December 1943. Venona Collection, Provisional Box #1.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

On 8 Oct 1943, Coudert reported that the IBM section at Arlington Hall had completed runs on the first and last five groups of 10,000 [redacted] (Trade) messages.[57] Presumably Hallock and the others made their discoveries in this compilation, for, "The machine runs which Lt. Coudert has received have brought to light unmistakable depth for pairs of messages, and have shown some interesting relationships between groups in various positions."[58] Thus the core secret of Venona had been exposed on or about 15 Oct 1943: messages could be matched and a depth of two found, that is, somehow or other the Russians were using the same additive (key) twice. In the end, during the Venona era, this was understood to mean that the US–UK was faced with a one-time pad additive system but for which duplicate copies of some pads had been made, and the Russian code clerks were using these without realizing it. Therefore it was not, or rather some of it was not, truly one-time.

The credit for this discovery has been variously given and claimed. Lt. Hallock, Miss Berry, Frank Lewis and Lt. Karl Elmquist all have a claim. Gene Grabeel says that Frank Lewis found the first matches: she recalls the event very well and the excitement in the unit (nonetheless she noted that Lt. Hallock could have been behind it). We quote from a report that Lt. Hallock wrote in August 1944.[59]

[redacted]

Because this first break into Russian diplomatic systems is so important to the history of U.S. cryptology, it seems useful to see just how the credit should be shared. Cecil Phillips offers this account, based on his discussions with some of the participants and his review of the documentary evidence:

> *As the only real cryptanalyst on the problem, Hallock probably initiated the work of machine punching and processing the 10,000 message beginnings and endings —fortuitously, almost certainly all or the bulk of it from Washington to Moscow and Moscow to Washington Trade messages of 1942 and the first part of 1943. Had this been done a year later with the last half of 1943 and first half of 1944 traffic, the results would have been negative. Hallock may have begun his work on the Russian problem in consultation with Mrs. Feinstein, who was one of the*

[57]See Weekly Report of B–III–b–9, 8 Oct 1943. NSA Archives, CBTB 34, in a folder of B–III reports for Oct–Dec 1943.

[58]Ibid. See weekly report of BIII Research unit, 15 Oct 1943.

[59]See "ZYT Report–6/8/44" signed by Lt. Hallock. Venona Collection, Provisional box #1. Hallock is probably the author of a 15 March 1944 report on ZYT. Same folder.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

> *senior analysts in the technical group from which he was on loan, but she did not come to the section on a permanent basis until after the first depths were found in October 1943; or he could have consulted with Mary Jo Dunning, who was the punched card processing expert (as was Al Small).*
>
> *Frank Lewis and Lt. Elmquist came to the section to look at the hits Hallock had found and discovered that many messages before and after the seven long hits were also in depth. This would have been the real bonanza and is the kind of event that would have been reported to Kullback.*
>
> *This success probably brought Mrs. Feinstein, Mary Jo Dunning and Burton Phillips onto the problem. From there, this team went on to discover the additive nature of the first two digits, and the nature of the opening stereotype in multi-part messages. Hallock might have played a role in these latter discoveries, but I am inclined to think not, because he was busy trying to find depths greater than two.*[60]

Even before these discoveries had been made, the Russian unit had begun a major buildup of its regular workforce (Hallock and some of his associates were temporary consultants to Lt. Coudert). By mid-November 1943, the permanent party numbered 30 (eight had arrived within a week). Coudert projected a force of 79 by the end of the year and 100 by the end of January 1944.[61]

Beginning the week of 8 October 1943, Coudert had started an expanded training program for his unit. This is a milestone in the history of the Russian problem. Coudert had earlier introduced his people to the target country by teaching an area studies course on the Soviet Union. The new training program included: twelve people taking a cryptanalysis course that consisted of three half-hour lectures and six hours of study per week; six people taking a Russian language course (taught by Lt. Coudert) consisting of three hours of instruction and six hours of study per week.[62]

Building on Lt. Hallock's discovery, the unit continued to find matches in the traffic. The cooperation with the Navy proceeded. Lt. Coudert's final report as OIC of the Russian unit, 19 Nov 1943, gives a good summary of this:[63]

> *In the (Trade) system, work has been devoted mainly to finding further matches between series of initial digraphs. A considerable number have been found. Many of them were between ..... Washington–Moscow and Portland–Moscow.*
>
> *These matches give a basis for additional overlaps. Nowhere, however, do we have a depth of more than two, and evidently some other means will have to be found to achieve an adequate depth.*

---

[60]Cecil Phillips's sources include Captain Bill Smith — in the summer of 1944, Smith (who had replaced Lt. Coudert in late Nov 43) described these events to Cecil. Smith in turn had learned this information from Frank Rowlett as part of his in-briefing. Bill Smith's story about the difficulties between Rowlett and Kullback over the work of Lewis and Elmquist "is almost certainly true because neither one of them set foot in the Russian section for some years after." Cecil continues that, "Smith also told me that Burton Phillips proved that the first two digits of the indicator were from the second key group on the page. Hallock's account attributes the discovery of the opening stereotype in multi-part messages to Mrs. Feinstein and Mary Jo Dunning — who often worked as a three person team with Burton Phillips."

[61]See the B–III weekly reports cited above; also the file "Correspondence of the General C/A Branch 1943–1945 in the CCH Collection at IV.c.3.3.

[62]Ibid. See B–III–b–9 report for week ending 8 Oct 1943. I do not know who gave the C/A lectures. Coudert's Russian language students, the first of many thousands, later included Trudi Levenger and Bill Doherty (per recollections of Mr. Coudert and Cecil Phillips).

[63]Ibid. See B–III–b–9 report 19 Nov 1943

> *Lt. Hall and Miss Clarke of the Navy visited (us) on 16 November. They were informed of the recent developments in the (Trade) system. Lt. Hall described the work done by the Navy on radio traffic.*
>
> *A frequency list based on 10,018 words from Russian plain text messages was received from USN.*[64]

K. UK Work on the Russian Problem 1930s–1944

The Official History, British Intelligence in the Second World War, by Professor F.H. Hinsley (and others) contains this statement about UK work on the Russian problem:

> *All work on Russian codes and ciphers was stopped from 22 June 1941, the day on which Germany attacked Russia, except that, to meet the need for daily appreciations of the weather on the eastern front, the Russian meteorological cypher was read again for a period beginning in October 1942.*[65]

The matter is more complicated than that and no definitive statement seems possible.

During the 1920s and 1930s, GC&CS (now GCHQ) had worked Russian diplomatic, Comintern and military traffic. The Comintern (Communist International) traffic, exploited from 1930–1937, is known as Mask.[66] The British and Indian Army intercepted Russian military traffic from sites in the Middle East and India. We have seen that GC&CS had a body of Russian military and NKVD crypto material, obtained from the Finns by Colonel Tiltman in 1940.[67] Russian Diplomatic traffic to and from London, which included the KGB and GRU traffic, was passed on international commercial circuits and, from later 1940, on national circuits too. According to the GCHQ account:

> *Few governments allowed the establishment of a national link from an embassy. London unfortunately was an exception to this and the Soviet Embassy was not only allowed but even helped to set up its own radio links with Moscow*[68]

(b)(3)-P.L. 86-36

Therefore, the GRU, and by 1941 the KGB, had a dual system for communications, ILC and NDC. The former could be covered by [redacted] copy, the latter required intercept — at a time when the wartime demands had to be given first priority. It is difficult to tell what was collected because most of the intercept and message logs no longer exist. But it is certain that nothing could be read at that time (actually 1939–41 Venona material hasn't ever been exploitable.) We return to the murky events of 1941. Professor Hinsley suggests that all cryptanalytic work on the Russian target ended on 22 June 1941 when the Germans attacked Russia, but he does not say that collection stopped. Field Marshal Sir John Dill, the senior military representative in Washington of the Prime Minister and British Chiefs of Staff, told General Marshall in December 1942 that, "in June 1941, upon the

[64]The Navy's work on radio traffic probably refers to "The Blue Caesar" series of reports on Russian military radio nets in the Far East. Commander Taecker prepared the Russian word frequency list using Russian plaintext that the Army had given him.

[65]London, HMSO, 1979. Volume One, page 199. Professor Hinsley served at Bletchley Park during the war.

[66][redacted]

[67]See the subsection on the Sinkov mission to the UK in 1941, above. In some notes written in 1951, Oliver Kirby, then heading the Russian problem at AFSA, wrote that, "no Comint center, allied or foreign, has read any Russian Armed Forces high level additive traffic since early 1940 when the Russians introduced the secure cryptographic systems which they continue to use" Perhaps a reference to British success before early 1940.

[68]"Soviet 'Diplomatic' Traffic on the London Link 1940–1949: A Survey" GCHQ. 3/NBF/C22, 17 Feb 1975. Venona collection, box 012, folder: S/NBF/C.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

German invasion of Russia, Y Board decided to stop working Russian service traffic." (emphasis added) The Y Board made high level Sigint policy, so this represented a national decision.[69] However, the Russian section at GC&CS was not closed down until December 1941, six months after the reported date of these decisions.[70]

Sir Peter Marychurch told me that "C" (that is Sir Stewart Menzies, Chief of the Secret Service and titular head of GC&CS) gave the order to stop working the Russian problem in early 1942.[71] We also have an outline of these events from Hugh Alexander, onetime head of cryptanalytic research at GCHQ, which included the Venona program:[72]

> *A. General Order in 1941/42, implemented by Tiltman to stop work on Russian and destroy material.*
>
> *B. Cancellation of this order so far as service material went in Jan 1945 with the setting up of Pritchard's covert party at Sloane Square.*
>
> *C. Continued destruction, or non-interception of (Russian Diplomatic) until Sloane Square party returned to GCHQ in July 1945 and work on Russian became overt.*

The reference to Colonel (later Brigadier) John Tiltman concerns his statement that he ordered the destruction of Russian Diplomatic traffic. But the date(s) seem unclear—did Tiltman refer to housecleaning after 22 June 1941 to get rid of unreadable traffic of a country no longer a Sigint target? Or did he mean that collection continued and at some later time, perhaps 1945, he pitched the accumulation of the still unreadable traffic? In an interview in 1979, in which, incredibly, the most important part had been erased from the tape before transcription, Tiltman said this:

> *(Missing portion) Russian traffic to be destroyed. We had a room full of it. Not being sorted you know.*
>
> *I don't know whether I told you or not, if I mentioned the fact that years afterward when we were talking about Philby (someone) said to me in the middle of a meeting, 'If you hadn't taken that action the whole future of the world would have been changed'*
>
> *I was able to take (blame?) even though I didn't have to. We weren't sorting it, couldn't do anything so we just threw the lot away. And we regretted it afterward.*[73]

Whatever may have happened (and we speculate on this in Chapter IV), the UK was in fact working Russian targets by 1943. At a meeting that year between "C" and the Director General of the Security Service, "C" decided that some Russian systems should be worked[74] From March 1942, the Metropolitan Police and the Radio Security Service (RSS was first a part of the Security Service, MI–5, and transferred to the Secret Service, MI–6, and in either case was an intercept asset of GC&CS) discovered extensive Russian illicit radio links, apparently GRU, KGB and Comintern. "In 1943 it was decided at a high level to drop coverage (of KGB and

[69]From notes in author's collection. A copy of the Dill letter is almost certainly in the collection of G–2 Special Branch papers, CCH Collection.

[70] [redacted]

[71]Interview with Sir Peter Marychurch and Mr Howard Vincent by Benson at GCHQ, 5 May 1992.

[72]Message, 15 Feb 1965 from GCHQ to SUKLO Washington, Exclusive for Parker from Alexander. Venona collection, #3337, Box 13, Callahan folder #2.

[73]Tiltman interview by Dave Goodman and R.L. Benson, 30 Jan 1979, OH 01–79, CCH Collection. Cecil Phillips says that Tiltman told him, in 1946, that Russian Diplomatic had been collected but destroyed — it is Cecil's impression that Tiltman meant collection continued after 1941.

[74]Lou Maddison, GCHQ archivist. Discussions with Benson at GCHQ, 6 May 1992.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

GRU) and concentrate on (Comintern), the chance of success in the Comintern field being considered much higher."[75] The Radio Security Service completely took over the intercept from the police in May/June 1943 and a covert section of GC&CS was established in London to work the material. Professor Scott headed this section and the decrypts are known as ISCOT. The first ISCOT translation, issued 21 Jan 1944, is of a 12 July 1943 message. The material was exploited through the end of the war, some in near real-time, and Scott's group issued 1484 translations. The ISCOT material, though called Comintern, looks similar to some GRU illicit and mainly concerns the fighting and intelligence gathering of Russian controlled Partisan forces in German–occupied Europe, especially Yugoslavia, Poland and Italy.[76]

It was not broken until the 1960s. The ISCOT material, of potentially great significance to UK diplomatic and military policy, seems not to have been shared with the U.S., and as we have seen, the U.S. did not share its Russian Sigint effort either.

In later 1944, GC&CS established a special section to work Russian internal non-Morse traffic (military and civil circuits).[78] Presumably this was Pritchard's covert party, working at Sloane Square in January 1945, mentioned above in Hugh Alexander's message.

The timing of all this can be considered in light of the formalization of a US–UK Sigint relationship in 1943, a relationship which has been continuously in effect for 50 years.

In April–June 1943, Colonel Al McCormack and Major Telford Taylor of G–2 Special Branch , and William F. Friedman of Arlington Hall visited GC&CS and were shown almost everything, especially the methods for exploiting and disseminating the Sigint derived from the German Enigma cipher machine. This visit followed, or coincided with, the signing of an agreement between Major General George V. Strong, Assistant Chief of Staff, G–2 and Commander Edward J. Travis, head of GC&CS, that called for a full exchange on intercept and solution data concerning Axis communications. General Strong advised General Marshall, the Army Chief of Staff, that the agreement "does not cover traffic from non-service enemy or neutral sources", an important distinction that would allow each country, in good faith, not to exchange information on Russian diplomatic, Trade or intelligence service traffic.[79]

During Aug–Sep 1943, Roger Randolph of G–2 Special Branch visited the GC&CS Diplomatic operation at Berkeley Street. He was shown almost everything, materials that could have been excluded from the agreement. In his report he puts the Russian problem under "Miscellaneous Matters" and had only this to say:

---

[75]

[76]This material is of great historic interest and some of it relevant today, e.g. the traffic concerning Slovene, Serb and Croatian independence movements. Some ISCOT messages have information useful to the history of the Holocaust.

[77]I don't know how this squares with the decision to concentrate on Comintern, though that decision may have related more to processing than to intercept.

[78]Discussions with Lou Maddison at GCHQ, 6 May 1992.

[79]An original signature copy of the Strong–Travis agreement is in the CCH Collection at XI.B., Box 2 of the Carter Clarke papers. The dating of the agreement depends on how one decides who made the final decision to validate the agreement. The signature page shows 1 March 1943; the front page of the agreement is marked 17 May 1943; General Strong sent it to General Marshall on 10 June; and on 15 June 1943 Colonel Otto L. Nelson, Secretary of the General Staff approved it on behalf of the Secretary of War and the Chief of Staff. Some copies of the agreement show that Travis signed on behalf of the British Chiefs of Staff. Technically, Commander Travis was a deputy director of GC&CS (for military/naval sigint) and Commander Alistair Denniston was the other deputy director for civil Sigint (Dip, commercial). "C" had the title of Director General of GC&CS.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

II. THE BEGINNING OF THE RUSSIAN PROBLEM, FEB–DEC 1943

> *Prior to 1941 Russian diplomatic traffic was studied. The conclusion was reached that it was one-time pad and accordingly the research was abandoned. At the present time Russian diplomatic traffic is not being analyzed and none of it is being read.*[80]

A final note on the comparison of the US and UK Russian programs of the time. We know that both countries closely cooperated on the Japanese military attache systems, exchanging traffic and translations of messages. In Sam Snyder's report of 15 Feb 1943, he says that packet BRZ #200, sent to London on 12 February, included a note from him to GC&CS regarding the transmission of Russian codes in JMA. His report of 12 April says that package 268 sent to London on 9 April contained "a note on Russian code messages."[81]

[80]Venona collection, box D101, in a folder marked NSA Technical Library S–7289, a series of papers on individual target desks at Berkeley Street. Note that Randolph did not say that GC&CS had stopped collecting Russian Dip traffic.

[81]See the binder labelled SSS Diary 1940–1944 (JMA), in the Snyder papers, box 2, CCH Collection at XI.K.2. Snyder surely did not mean to tell the British that Arlington Hall had started a covert Russian program. But by drawing attention to these JMA messages, Mr. Snyder could have been, accidentally, contributing to the controversy surrounding the security of the Zubko/Grabeel program.

III. The Bill Smith Era Nov 1943–46

A. Change of Command

Early leaders of the Russian program: Captain Coudert receives award from General Corderman, Captain Bill Smith on the right.

On 22 November 1943, Captain William B.S. Smith replaced Lt. Ferdinand Coudert as head of the Russian unit. Smith came to Arlington Hall as a civilian in 1942, and soon thereafter received a direct commission into the Signal Corps. Smith and Coudert had been classmates at Harvard. After graduation Smith took a position with the Columbia University Press, eventually becoming an editor of the Columbia Gazetteer and the famous one-volume encyclopedia that went through many editions (although an editor, Smith himself wrote some of the entries in the encyclopedia, especially on religion and linguistics—Smith knew French and the rare Breton dialect). Smith originally had worked on the French problem at Arlington Hall.[1]

Lt. Coudert remained as deputy chief of the unit and linguistic assistant; Lt. Hallock, who had made the fundamental discovery about the Russian Diplomatic systems, stayed on as technical assistant. Coudert, happy to be free from day to day administrative duties, turned to a wider range of translation activities, and he continued to teach Russian language and area studies to members of the unit, while founding other language training programs as well.[2]

The Russian unit now consisted of 34 people and had been re-designated B–III–E, the Special Problems subsection. This represented a fairly substantial commitment of resources and the unit grew steadily during the

[1] Smith, born in 1909, had a B.A. from Harvard and an M.A. from Columbia. He had two stints with the Columbia University Press, 1932–35 and 1940–42. In between he was an instructor at Providence College. The French problem at Arlington Hall was actually several problems, based on crypt system and target entity—Free French, Vichy and Swiss [redacted]

[2] Mr. Coudert told me that he helped the Balkan Section on Bulgarian and Serbo-Croatian material (including the translation of a letter to the U.S. from General Mihailovich, the Chetnik leader). Also, see Volume 2 of the History of SSA, p. 190–191 that states, "The Slavic languages were at first represented by Captain Ferdinand Coudert, who did much of the preliminary research", and that Captain Coudert "devised linguistic tests to determine the fitness of the personnel for this sort of work and began a training program in the minor Slavic languages."

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

next year, in spite of the demands for ever more people to work the Japanese Army systems and to begin a significant German military program. In an interesting think paper written at the request of Colonel Cook, head of B Division (Sigint production), R.P. Oliver made this comment:

> *The alignment of powers in the next war cannot now be predicted. A few very general considerations, which must suggest that it is imperative never to relax work on Russian and Chinese systems, are all that can be seen with any clarity by the contemporary eye.*[3]

B. Developments During 1944

Captain Smith immediately began reorganizing the cryptanalytic efforts, with particular attention to the Russian Diplomatic problem. He set up procedures for message logging which, with minor changes, would continue throughout the Venona period. He established the principles of "masterblocking"—a procedure in which messages are recorded in order of original encipherment with an arbitrary master block or pad number assigned. Smith discovered that if messages were ordered first by file date and time, masterblocking would be straightforward, but messages into Moscow had to be ordered by external serial number.[4]

Smith stopped the effort against some of the Russian Diplomatic systems in favor of concentrating on the Trade systems where Lt. Hallock had found the depths: Miss Berry ceased her work on [redacted] (later found to be GRU), Miss Boake ended her study of [redacted] (later found to be GRU–Naval) and the Navy may have been invited to look into the other Dip system (later found to be the true Dip Consular system [redacted]). We have no contemporary record that much had been done on the [redacted] systems, later identified as KGB and which would be the heart of Venona. Work on all these systems shut down until July 1944, with all attention given to the Trade messages. Cryptanalytically this made good sense. It represented by far the greatest volume of Russian Dip and a small but vital beginning had already been made in breaking it—the discovery of depths, that the same key appeared at least twice for a large number of messages.

Still, in retrospect, some of the objectives or methods seem unclear. What would be called the [redacted] systems, that is the messages of the Soviet Purchasing Commission to and from the Ministry of Trade in Moscow, had been identified right away, by Lt. Zubko as just that. The intelligence value of these messages, even if read in real time (and none could be read at all during the first year of the Russian problem), could not have been expected to be high. Certainly the messages on the U.S.–Moscow lanes would have been expected to contain information we already knew: endless lists of parts, equipment, goods; shipping data; terms and dates. We were openly supplying the Russians and working out with them all the details of delivery and shipment. Yet, in a report of 30 June 1944 on the Blue Problem (Blue having become the codeword for the Russian problem) we read that the major cryptanalytic successes are to be found in the study of ZYT (at that time the term for [redacted] that is Trade), a diplomatic system, "presumably carrying intelligence of a high grade and used by many stations."[5] Probably the only conclusion we can make is that everyone involved saw this as a

[3] Paper, no heading or signature, with handwritten covering note, 4 Dec 1943. Oliver's paper is quite interesting as it concerns continuing oversight and collection of unworked systems during a time of transition.
[4] From the Hallock reports and Cecil Phillips
[5] Supplement to the Annual Report of B Branch, 1 July 1943 to 30 June 1944 : The Blue Problem. CCH Collection, IV.c.5.6.

pure cryptanalytic problem, which it would remain until Dip systems became readable—then the consumers would decide what had intelligence value and the problem would go from there.[6]

Following Hallock's discovery about re-use of key, the unit found several thousand pages of re-use, but no usage more than a second time, that is, a depth of two only could be found. This was discouraging to the cryptanalysts at that time because the conventional wisdom was that re-uses had to be greater than two to be solvable.

This attack, completed in March 1944, failed to produce any results. Hallock also considered a possible attack in which tentative key groups from the existing re-uses might be tested against other messages. There is no evidence that he tried this at the time, but in later work all solved key was tested against all messages.[7]

Meanwhile effort continued to fully explain the message indicator of the messages where re-use had been found and to recover some code groups from the re-uses already found. About half of the case of re-use did not have the same key page number, but in all cases the first two digits of the indicator were identical if the messages were in depth from the beginning. The Japanese had suggested that these two digits were some form of row and column coordinates, but Hallock's group had also discovered that when these digits were subtracted from the first two digits of the third group, the resulting dinome was not randomly distributed. According to Captain Smith (in a discussion with Cecil Phillips in 1944) Burton Phillips concluded that the two digits in the indicator were key and that the non random result was two digits of code. While we have no information as to how he arrived at this conclusion, it was clearly proven by the next major success on the depths—the discovery of self-checking code groups for numbers at the start of many messages. Miss Berry recalled that she either noticed or identified some aspect of the Trade indicator in later 1943. Since Miss Berry was working closely with Burton Phillips at the time, her discovery may have related to the two digits of key in the indicator which Burton Phillips apparently confirmed.[8]

It had been observed earlier that the code digraph among the long messages which appeared to be parts were different from shorter messages. These messages were almost uniformly about four pages or 240 groups in length, and the non-random digits derived by subtracting the first two digits of the indicator from the third usually began with a zero in the second and succeeding members. Further, it had been observed that the digraph was 01 for a long sequence and later became 02. According to Hallock's reports, this led Mrs. Feinstein to suggest that this might be representation of some continuation message number of the previous message. This proved to be true—and even better—it turned out to be a representation of the external number of the preceding message—providing an almost certain four group crib into the first four groups of the message. At about the

[6] Throughout the research for this study we asked veterans of the problem if they had ever been briefed on what to expect in the traffic, particularly if they had been directed to look for probable KGB or GRU systems. No one recalled ever having been told what to look for—from a content standpoint—and no one ever had a briefing from G–2 or the FBI for example about the Russian intelligence services. It was seen as a cryptanalytic problem—the nature of the traffic would be revealed by breaking into it and reading it.

[7] Cecil Phillips provided, and largely wrote up, all the technical information in this paragraph and others in this section. He is a primary source for the history of Venona.

[8] Cecil Phillips; also Cecil's discussions in 1992 with Carrie Berry.

same time the code groups for numbers were found to be numeric code groups of a clear self-checking variety—which enabled virtually instantaneous determination of the form of the 1000 code groups used to express numbers.[9]

The Russian unit moved in January 1944, into a larger work area, but one typical of most of the work areas of Arlington Hall. They occupied an open area measuring about 50 x 50 in the back of the second floor of the B Building. Their space was separated from the rest of the open wing, occupied by the weather section, by large wooden screens that were some seven feet high and four to six feet wide. A small opening between the screens provided the entrance to the "office". Captain Smith sat at a long table to the left of this tiny entrance, with his back to the partitions, seated so that he could watch everyone at work and coming and going (as they had to squeeze by him). This was truly another era— the section had only a couple of desks, otherwise everyone sat two-by-two at tables seated on old, cast-off and unmatched chairs. The unit had just two or three standard typewriters and one Russian typewriter. Everything except paper and pencils was in short supply. The place was not airconditioned. The unit, officers and civilians, worked a six day week (but were not paid a full day's pay for Saturdays).

Security was especially tight in the Russian section. Those studying Russian under Lt. Coudert had to lock up their language books and dictionaries; maps of Russia came off the walls at the end of the day. Smith and Coudert admonished everyone to talk in a low voice and to avoid discussing their work with anyone else at Arlington Hall. At the end of the day all the cabinets were locked and the classified or target-revealing trash put in a special container.[10]

Unfortunately the KGB seems to have already heard about the Russian problem at Arlington Hall and their stooges were hard at work trying to learn the details.

C. Lauchlin Currie, the Silvermaster Ring and the KGB: Spring 1944

In November 1945, Elizabeth Bentley, a veteran KGB agent, gave the FBI a 107 page statement (See section I. of this chapter). Among the many startling revelations about KGB espionage in the the U.S. was this:

> *During this same period I became aware of the fact that Lauchlin Currie was friendly with the SILVERMASTERS and was particularly friendly with GEORGE SILVERMAN. To the best of my recollection, Currie did not supply SILVERMAN or the SILVERMASTERS with any documents, but used to inform SILVERMAN orally on certain various matters. As an example of the information orally furnished SILVERMAN, I recall one occasion when CURRIE informed him that the United States was on the verge of breaking the Soviet code.*[11]

Unfortunately, Miss Bentley did not give a date for this incident, nor can a date be determined by the phrase "During this same period". However, as later investigation would show, it was most likely March or April 1944.

Currie, born in Nova Scotia, was a prominent academic economist connected to the Roosevelt administration from 1934–45. He received a PhD from Harvard in 1931, became a U.S. citizen in 1934 and taught at Harvard and the Fletcher School of Law and Diplomacy. In 1934 Treasury Secretary Morgenthau

[9] Cecil Phillips. Cecil believes that at this time, while Burton Phillips, Genevieve Feinstein, Mary Jo Dunning and Captain Smith were making these discoveries, Gene Grabeel was supervising the rest of the unit, carrying out the most basic cryptanalytic tasks upon which the success of the others was built.

[10] As recalled by Cecil Phillips, Gene Grabeel, Ferdinand Coudert; also see the report on The Blue Problem, previously cited. Miss Grabeel recalled that Lt. Coudert was especially concerned with security and talked to people often about it—we should also note that Coudert made a lasting impression, entirely favorable, on those who worked for and with him.

[11] Statement signed 30 November 1945, NY Field Office, FBI. A copy of this statement is in the Venona collection.

appointed him as a senior analyst for the Treasury Department; in 1939 he became an administrative assistant and economic advisor to President Roosevelt. He held that position from 1939–41 and intermittently thereafter, and during the war years had at least one stint as temporary stand-in for Harry Hopkins. He performed various special missions during the war including a fact finding mission to China.

In 1947 Currie denied to the FBI that he had told Silverman that the U.S. was on the verge of breaking the Soviet code. Currie did say that he might have heard about such codebreaking developments in view of his contacts and position. He said that he would have had no problem telling Silverman that type of information but did not recall having done so (Silverman, an employee of the Air Staff at the Pentagon had a clearance, though no known official access to Sigint— and obviously no need to know regarding the Russian problem). In a December 1952 appearance before a Federal Grand Jury in connection with another matter (not involving himself), Currie was asked about the codebreaking matter. He denied ever discussing this with anyone. When reminded of his previous statements to the FBI about Silverman, he said that he would not have told Silverman such information (but he didn't say that he knew that information anyway).

In her 1951 book Out of Bondage, Miss Bentley did not mention the codebreaking incident. However, she made a brief reference to it in her six part series in the New York Daily Mirror. Upon reinterview by the FBI, Miss Bentley dated the incident to the Spring of 1944. She recalled the considerable rushing about by Currie, Silverman and Silvermaster to get this information to the Russians and then to follow up. At that time Silvermaster controlled a major KGB net; Bentley was an auxiliary agent handler and the courier between Silvermaster and the KGB. Bentley said that she verbally reported to her KGB superior, "Bill", the information that some agency of the U.S. government was on the verge of breaking the Soviet code and "they almost had it". Bill then said to her, "Well is it a trap or isn't it a trap?" He told her that her network had the "assignment and duty" to determine the particular code the Americans were about to break. Miss Bentley said that while she and the Silvermaster net worked on this for a time, they never learned which code was about to be broken (nor did they learn anything else about the U.S. Russian Sigint program—at least Miss Bentley could give the FBI no further information on this matter.).[12]

Venona would prove that Miss Bentley's statements about KGB activities in the U.S. were extremely accurate. Nonetheless, her Currie story might be considered a bit slim on detail, and it has not been found in Venona. However, the FBI found two independent witnesses. One, a senior government official (name withheld) who worked closely with Currie during the war, said that Currie told him that he (Currie) had revealed to the Russians that the U.S. had "broken the Soviet Diplomatic code". Currie was disturbed that the U.S. had done such a thing, and because he believed it wrong, he said that he had "tipped off" the Russians.

In later discussions with the FBI this official recalled his conversation with Currie in greater detail, placing it in the Spring of 1944 (though he said it could possibly have been as late as Fall 1944). The official reported that Currie raised this matter by telling him that he knew of a very hush-hush matter, too sensitive to talk about. Currie then proceeded to tell him that he had learned that the U.S. had broken the Soviet Diplomatic code and that this was a terrible thing to do to any ally "and indicated our lack of trust in the Russians." Currie said that he had fixed this by telling the Russians, while assuring them that he, Currie, did not approve of such activities. Currie said that by his actions he had prevented the sowing of seeds of distrust between allies. Currie did not tell this official how he had learned about this and gave no details about the code that might be involved. The

(b)(3)-P.L. 86-36

official rebuked Currie. The official said that he had later described this incident to Frank Wisner of CIA and to members and staffers of the House Committee on Un-American Activities including Robert Stripling, Ben Mandel and Richard Nixon.

A second person associated with Currie during that time recalled that Currie said that the U.S. had broken the Soviet code. But that source said that her recollections were too vague for her to be good witness in any proceedings.

The FBI contacted NSA for assistance in this matter. General Ralph J. Canine, Director, NSA told the Bureau on 9 Dec 1953 that to his knowledge no Russian codes had been broken in 1942 or 1943. In a memo of 25 January 1954 General Canine told the FBI that the Army and Navy made no decryptions of Russian systems until 1945. On 12 Feb 1954, the Washington Field Office advised Bureau headquarters that:

> *It has been determined by NSA that in 1943 work on Soviet codes was initiated by both the Army and the Navy and that in early 1944 limited success was had with one Soviet system not strictly a diplomatic code. It was also ascertained that decrypts of messages were shown to President Roosevelt by a United States Naval Officer whose duty it was to take the decrypts to the White House and that Currie could have learned of the contents of some of them in that manner. For your information, NSA is making efforts to identify the Naval Officer whose duty it was to take the decrypts to the White House.*

NSA was not able to make this identification.

The Agency could have done better, in the Currie case and in the Weisband case, as we will discuss in a later part of this study. Suffice it to say that the FBI interviewed a lot of officers who had been in liaison with the White House, including Colonel Frank McCarthy, former Secretary of the Army General Staff and (later producer of the movie "Patton") but found very little. One officer, however, reported that daily summaries of Russian decrypts had not been prepared , "for this code had not been broken sufficiently ".[13]

Did the KGB react to Lauchlin Currie's information?

D. May Day 1944

On 1 May 1944, the KGB changed the indicator system for its encrypted international communications, that is for the enciphered code used by the Residencies and the Moscow Center. This change had been made on short notice although that would not be known until the Venona breakthrough, at which time the following message, from Moscow "To all Residents", dated 25 April 1944, was decrypted and translated:

(b)(3)-P.L. 86-36

[13] Ibid. My point is this: In the early 1950s, many people at NSA could have told the Bureau exactly what was going on in the Russian program during 1943–1944. Carter Clarke [redacted] could have helped. The lead suggested by NSA—to search for a naval officer who gave Sigint to the President—was preposterous and cannot be seen as anything other than misleading. I have not been able to find NSA records on any of this. AFSA had been similarly unhelpful to the Bureau in the Weisband espionage case—see Chapter VII.

From 1 May, instead of the method of setting up the indicator group in effect at the present time, for the determination of the reciphering table enter in clear the beginning of the cipher text the first group of the table with which the leaf of the pad (on the occasion?) begins. The recipherment itself begins with the second group of the table. At the end of the cipher text enter, likewise in the clear, the group following upon the last used group of the (additive key) (the second indicator group). If the recipherment ends with the last group of a table, enter the first group of the following table, ----------[note by RLB: thereafter some 89 groups of the message could not be exploited][14]

Cecil Phillips has observed that this indicator change was the KGB cryptographers second most important contribution to the cryptanalysts at Arlington Hall (first place going to the original flaw: the manufacture of extra sets of 'one time' key pads). The change had to do with the 'indicator' that showed what key page, from the pad book, was being used by the message sender. The timing is such that it suggests some connection to Currie and Bentley getting the word to the KGB that the Russian Diplomatic code was about to be broken. As a security measure it doesn't make much sense, but as the change was introduced in such a hurry, it does arouse suspicion. In any case, the KGB cryptographic directorate could have made the change merely to be able to tell Beria (who presumably would not have known the difference) that something was being done in the face of the information that the KGB New York might have told the Center when they got the report from Bentley (thru many KGB intermediaries in Washington and New York). That something does not make sense cannot be taken as proof or disproof.

Quite possibly, the indicator change was made for reasons other than the incomplete, and at that time inaccurate, information from Currie.

The indicator change on May Day meant the replacement of a fairly simple 2 digit key page indicator which had been in use for at least four years with a free 5-digit additive group from the key pages at the start and end of each message. The earlier system, the one replaced, and which during the Venona period would be called [redacted] by US–UK, provided a key page number in the last or next to last group—derived by subtracting a pair of digits representing units and tens digits of group count (which occurred as the first two digits of the indicator) from the third and fourth digits of the indicator group.[15]

The new indicator system resisted solution for about six months. During this period, Miss Berry and others tried all the conventional means of indicator solution—mostly subtracting one message group from another, which had been the basis for a number of indicator systems up to that time. None of these attacks produced any results.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[14] This message, a circular, was sent by the Center to the KGB stations in Havana, New York, Mexico City, Ottawa, San Francisco; the same message must have gone to the other Residents too (e.g. London) but in a message(s) that has not been broken. The message was translated by Meredith Gardner at AFSA by 1950, but not translated and reissued in later years (as most of Mr. Gardner's early translations were).

[15] Cecil Phillips provided all the technical data in this section. During the course of the research, which was a joint project, Cecil wrote many short essays—on individual topics and for general overview. Here I cite, and almost copy verbatim, from his essays "May Day 1944" and [redacted]–The Beginning". These are held in the Venona Collection with other research files.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

III. THE BILL SMITH ERA NOV. 1943–1946

In late September or early October 1944, Cecil Phillips and Lucille Campbell, who had been recovering key on a Far Eastern NKVD troop system, undertook on a parttime basis the solution of the new system. Phillips, a 19 year old cryptanalyst, had been at Arlington Hall for a year, joining the organization after his sophomore year at the University of North Carolina.[16] He had joined the Russian problem on May Day 1944.

Cecil Phillips (top left) and Frank Lewis (lower left). They made fundamental breaks into the KGB system in 1944. Venona veterans Bill Lutwiniak (top center) and Paul Derthick (top right).

During much of the period described above, Lt. Hallock had been studying the biased key distributions found in depths, searching for clues as to how the key might have been produced. As the section's senior cryptanalyst, Genevieve Feinstein had been following Hallock's work and was well acquainted with his findings of key families. In mid-November 1944, Mrs. Feinstein, upon reviewing the studies of distribution made by Phillips-Campbell, observed that this looked like "free" key and ought to be tested against the Hypothetical

[16] Cecil Phillips had been a chemistry major at UNC. As he had been classified 4–F by Selective Service, his mother suggested that he go to summer school or get a job. He went to the U.S. Employment Service in Asheville to inquire if the government could use a chemistry student. The USES directed him to a Signal Corps lieutenant who was at the Post Office recruiting for Arlington Hall. The officer gave him a short written IQ type test. Within two weeks he was at Arlington Hall. He worked the Japanese weather problem most of his first year and transferred to the Russian problem on May Day 1944, the day the indicator change took place.

Additive Bank that the unit had recently produced by predicting the opening code in Trade messages, and then card punching the results to produce an index.

Genevieve Grotjan Feinstein, principal cryptanalyst in the 1944 break into the KGB cipher system.

"Free" key meant that the message text included as a first cipher group key taken from the opening group at the top of the pad page, in other words the cryptanalyst was "seeing" the opening group from a KGB one-time pad sheet. By knowing the true value of that opening group it would be possible to quickly look for matches by taking that true value and looking for the same value in another message (which might or might not be in the KGB system—more likely it would be in a Trade message). If that same value was found, in the right place in the message, then the cryptanalyst knew that the same pad page had been used twice. A match in a depth of two—enough for Arlington Hall to eventually break into the matched messages.

At the direction of Burton Phillips, Katurah McDonald and two clerks who worked for her began testing Mrs. Feinstein's hypothesis. The results were quick and dramatic, for the testing began to produce repeated opening code phrases in New York to Moscow KGB messages. Thus, the May Day indicator and the first reuse in [redacted] (the name that would be given to KGB systems) were found simultaneously. In a few days—and this is still in November 1944— several hundred pages of key reuse were found and the work on some of best parts of Venona began. But the nature of the [redacted] text was not apparent for two more years. Nonetheless this was the most important single cryptanalytic break in the whole history of Venona, and, like the fundamental discovery of reuse of key, has merited the naming of names.[17]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(6)

[17] In some of Meredith Gardner's notes, this breakthrough has been dated to Feb 1945 [redacted] GCHQ historian of Venona and a veteran of the program, used Mr. Gardner's date). We move it back to November 1944 based on Cecil Phillips' recollections and papers he reviewed about the attack on [redacted] the Russian consular system (and one of the Venona systems).

III. THE BILL SMITH ERA NOV. 1943–1946

E. Carter Clarke Delivers a Warning to Arlington Hall

General Carter W. Clarke.

We have discussed the activities of Lauchlin Currie and have outlined the story of the May Day cryptographic change. These could be related, but we cannot know. The third part of this story seems even less clear, but it needs to be recorded; and then we can try to summarize and offer some explanations for these events of 1944.

According to Frank Rowlett, who in 1944 headed the General Cryptanalytic Branch at Arlington Hall (which as discussed earlier meant all Sigint targets other than Japanese Army), Colonel Carter W. Clarke, head of G–2 Special Branch and controller of Army Sigint policy, visited him and Colonel Harold G. "Dink" Hayes, fairly soon after Hayes arrived at Arlington Hall, bringing an important warning from the War Department. We cannot put a date on this, except that it almost certainly took place in 1944. While Hayes had arrived at Arlington Hall in March, after heading Army cryptologic activities in North Africa and Italy, Mr. Rowlett could not really date the visit except to say that he "assumed" it was soon after Hayes "took command". Hayes took over the B Branch, the Sigint production organization, in which Rowlett was a principal subordinate at the beginning of April 1944, so perhaps the meeting was in April or May.

Clarke began by asking, "Tell me what you are doing on Russian?". Rowlett explained the Russian program. Clarke then turned to Hayes and said, "You haven't told me that you are doing anything on Russian, have you Dink?" To which Hayes replied, "No sir, I haven't" Clarke then said to Hayes, "You stop doing what you told me you were doing on Russian and Rowlett you keep on doing what you told me your outfit is doing on Russian." Clarke then explained that he was acting as a messenger for the War Department bringing an instruction from the White House, actually from Mrs. Roosevelt, that Arlington Hall was to stop working on Russian Diplomatic. Clarke described it as a cease and desist order, and they were to ignore that order. Clarke said no more, then or later, and the Russian program continued.[18]

We can only guess what lay behind Clarke's visit or exactly how the order reached him. Most likely he got the word from General George V. Strong, the G–2, acting on orders from either Secretary Stimson or Assistant Secretary John J. McCloy, probably the latter, as McCloy had oversight of Army intelligence programs and had a particular interest in Sigint. Lauchlin Currie had ready access to the White House, as an administrative assistant to the President and because of various special assignments. He sometimes sat in for Harry Hopkins, who had a number of illnesses during those years. Whether he "got to" or otherwise influenced the President or Mrs. Roosevelt on this matter is unknown; he could just as well have issued some verbal instructions to the War Department in the name of the President.

Instead of speculating along these lines, we conclude the Currie-May Day story with some suggestions about what Currie could have known about the Russian program:

- During 1944, the U.S. could not exploit the Russian Diplomatic code; no one in the know could have suggested that we were on the verge of a breakthrough until, at the earliest, later November 1944. Even then such a prediction would have been unlikely.
- However, the White House may have been informed by the War Department or Navy that the U.S. was working Russian systems and could have received some not very interesting translations from Russian military/police systems — but nothing from Diplomatic. Currie could have known about all this.
- Just as likely, Currie could have taken what he heard about the U.S. effort against Russian communications and leaped to some conclusions, given his almost certain knowledge of the extraordinary US–UK successes against Japanese and German communications.

In a later part in this study we will review some Venona decrypts relating to KGB access to the White House and the possible identification of Currie in the traffic.

[redacted]

[18] Rowlett interview by Benson, 14 Jan 1992, Sarasota, Florida; Rowlett interview by Hank Schorreck and others, 31 August 1976 and after, at NSA, CCH Collection, transcript of Rowlett interview.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

III. THE BILL SMITH ERA NOV. 1943–1946

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

[redacted]

G. Slow But Steady Progress at Arlington Hall and Nebraska Avenue 1944–1945

By the end of 1944, Captain Bill Smith's Russian unit at Arlington Hall had 18 cabinets full of diplomatic traffic, none of which had been read, representing about 150,000 messages in all the Russian Dip systems (including Trade) of which only 10% had been found to involve reuse of key, meaning that only the latter could potentially be solved. In the next 5 years, another 700,000 or so Russian Dip/Trade messages were collected, and about 15,000 of these also involved reuse.[25]

During 1944, the unit mostly worked Trade messages, which represented the bulk of the traffic, though as we have seen the major break in November was into what would later be recognized as KGB. That break had been made because the KGB changed its own indicator system on 1 May 1944. The KGB, though responsible for all cryptographic doctrine and production of all crypto systems, had not effected an indicator change in the other systems. From about July 1944, the systems that Smith had dropped 6 months before again came under active review. These included [redacted] and [redacted] the system identifiers later used for Consular, GRU–Naval, and GRU systems. The Navy continued its small but active inquiry into Russian Diplomatic systems, but always in consultation with the Army.

Captain Smith may have asked Commander Taecker to take over the study of [redacted] and [redacted] for some of the informal records of the time mention that the Navy had assigned a couple people to these systems. In late September 1944, Commander Taecker gave Smith a short technical report on [redacted] "drawn up by our people here (at Nebraska Avenue)".[26] Lt. Robert Carl was the Navy's principal analyst for [redacted]

The Navy's overall Russian program grew considerably during 1944. By June a 26 person unit at Nebraska Avenue was working the traffic and three small watches at field sites were intercepting naval, military and police traffic. In September, Ensign W.W. Moeschel was integrated into Arlington Hall to work military systems. During October–November, 20 officers reported to the Russian section after completing language training at the Navy's school at Boulder, Colorado. In November the Navy began publishing intelligence summaries of

[25] From Cecil Phillips paper, [redacted]–The Beginning
[26] Informal Memorandum for Captain William S. Smith, Signal Corps, 28 Sep 1944, signed by Cmdr C.H. Taecker. Venona Collection, Provisional Box #1, ZZH Folder #2.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

Russian decrypts four times per week.[27] In December, Commander Taecker left the unit, replaced by Lt. Commander G.L. Todd, like Taecker, a retired officer recalled to duty. Some internal organizational changes were made at this time to increase security and disguise the existence of the Russian program.[28]

In spite of the dramatic success at Arlington Hall in November 1944, only modest gains were made in 1945 against the Russian diplomatic systems. Nonetheless the work during that year laid the foundation for the Venona breakthrough of late 1946. Most of the effort went into getting [redacted] (KGB) code recovery and [redacted] (Trade) code recovery to a state where context could be obtained from the matches to obtain meaningful text. We must continually emphasize that the Arlington Hall Russian unit still had no clue to the real identity of [redacted] –at the time it was seen as a modest sized, in terms of traffic volume, world wide Russian Dip system that looked susceptible to full solution. No one knew what that solution would mean in terms of intelligence.

As an example of the difficulty of the work, as of 15 April 1945, it was not yet certain that the Green trade code was a two part code, this almost 18 months since Lt. Hallock and his team had found the first reuse in [redacted] As a further example of the slowness of the effort, by February 1946 only 35 [redacted] code groups had been identified, and a year later, though 2600 [redacted] code groups had been identified, only 320 had been given Russian meanings.[29] In other words, four years after the Russian program had begun, only 3.5 percent of the values in that KGB codebook could be read. At this point it seems useful to leap ahead to give some idea of what the Russian Dip systems looked like, with the understanding that Arlington Hall, at this point in our narrative, did not know any, or much, of this.

All the Russian systems passing as Dip used an enciphered code. For the KGB (the [redacted] systems) this meant a codebook of 9999 groups, 0001 thru 9999. System [redacted] used a book of that size, with the groups being enciphered by additive drawn from the one time code pads. We have seen how the Russians changed the indicator system, which meant the system for determining which page of the one time pad book was being used. The codebook also allowed the code clerk to spell out words that were not in the codebook, a vulnerability of the system.[30] This was a centralized cryptographic program—a department of the KGB drawing up different codebooks for the different organizations involved in the worldwide Dip communications nets.

That KGB cryptographic unit also prepared the one time code pads from which the additive was taken and added to the codegroups being transmitted. Obviously, the real security was in the onetime pad additive. The KGB professionals, if not their leader Beria, much less Stalin, surely did not believe that the codebooks themselves could always be protected given the fortunes of war. Nonetheless, it was KGB doctrine to very carefully protect those codebooks. Such a system could only be broken if the opposition cryptanalyst had the one time pads or knew how the pads were generated, and thus could replicate them. The generation scheme was never determined or replicated. The only hope lay in finding reuse of pad pages. This happened through successful matching, also called finding of depths or overlaps. All these terms can be used interchangeably. While we will discuss all this later, the reuse of pads was not what one would expect—carelessness by the code clerks. Instead, the break was possible because of what came to be called manufacturer's re-use, which meant that sometime after the German invasion of Russian (22 June 1941), the KGB's pad generating center

[27] Most of the decrypts were of naval and NKVD naval ("Coast Guard") traffic. No Dip had been solved by Army or Navy.
[28] OP–20–G Russian Language History
[29] Cecil Phillips' paper, RUD—The Beginning.
[30] But a vulnerability only if the security of the one time pad was breached. The spell table was a code within a code, but it existed to give the communicant a way to spell out words and thus get beyond the limitations of the vocabulary of the basic codebook. The spell table was not as such a COMSEC system.

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

manufactured extra sets of pads, probably because of the pressures of the rapid German advance and the emergency conditions. However, the re-use meant that one extra set of key pad was produced but only one extra set, thus creating a depth of two but no more. In other words, one time pad A should have been manufactured in two copies only, one for the user in the field and one for that user's headquarters element in Moscow. What happened was that a second set of pad A would be manufactured and issued to different communicants. In this example, Pad A might have been issued to KGB New York and the Center; the second set of Pad A might have been issued to the Soviet Government Purchasing Commission in Washington and the Ministry of Trade in Moscow. It was a matter of finding the match. No aspect of the Venona process would be more important than working the voluminous Trade traffic to look for depths with other more interesting (from the intelligence standpoint) systems and then to recover codebook vocabulary or values.

Work on the one part Red [redacted] (Trade) code was progressing fairly well by April 1945 (one part meant that the codebook was in strict alpha-numeric order, a big help for the bookbreaker). But almost all the work was concentrated on the first four groups of each pad page, a technique that took advantage of the vulnerable stereotyping in this class of traffic. During that April, Dr. Samuel P. Chew transferred into the Russian unit, after two years on the Japanese Army problem. Chew, who had been a Professor of English at the Citadel, the University of Wisconsin, and Oklahoma had joined Arlington Hall on 4 February 1943.[31] Dr. Chew was a tenacious cryptanalyst who attacked the Trade-Trade depths with enthusiasm and undoubtedly reinvigorated the Russian unit's Dip effort. In making this attack Chew discovered a form of stereotyping in Red Code Trade messages which made solution of any of these depths much more possible. The discovery that there was a pattern—later called the "item cycle"—in which commodities and shipment amounts were listed in an order and with sum checks made some text prediction reasonably practical. This added enormously to depth reading capability of Red code against Red code and Red code against Green code (also Trade or [redacted]—and against [redacted] (KGB) as well. In fact this discovery was a very major, some would say the most important, contribution to the Venona break.[32]

Fortuitously, the New York KGB messages would be matched primarily against the Washington to Moscow Trade messages—the messages with the most stereotyping ever found in any of the Dip systems.

In July 1945, Cecil Phillips discovered the explanation for the early 1942 Trade usage which had long been thought to be some form of local reuse. It turned out that each cipher (key) page was used in normal fashion and then reused in reverse, digit by digit, if the message was longer than one page but shorter than three pages. Thus the odd pages of a message were enciphered in normal fashion and the even pages in reverse. This gave rise to about 4000 pages of a peculiar form of depth, all in the Red Code. From this came the sub-problem known as the Red Reverse problem, staffed by a dozen or more new people made available to the unit at the end of the war against Japan. These depths had no promise of intelligence production but would be very useful in the Venona exploitation.[33]

---

[31] Interview of Dr. Chew by Benson and Phillips, 5 August 1992, Washington D.C. Dr. Chew told us that he had taken the Army's correspondence course in cryptanalysis before the war (as had Gloria Forbes and many others). However, he was recruited by Dr. Leslie Rutledge, who had joined Arlington Hall during 1942. Chew, a member of an old Anne Arundel County, Maryland family, graduated from St. John's College, Annapolis in 1931, and received a PhD from Harvard in 1937. Chew, Rutledge, Captain Bill Smith (head of the Russian problem at this point in our narrative) and Lt. Ferdinand Coudert (his predecessor) had all known each other at Harvard. During the war years, Chew, Smith and Rutledge shared a large house in Washington on Newark Street.

[32] All of this is from the Phillips paper cited above.

[33] Phillips paper and recollections; Mr. Phillips used reports dated 15 April 1945 and 15 August 1945, held in his study materials, Venona collection.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

III. THE BILL SMITH ERA NOV. 1943–1946

In April 1945, the unit completed the machine processes of matching key digraphs to find Trade-Trade depths. This produced a large number of reused pages. But this technique gave way to the Hypothetical Additive Bank because of the latter's potential for finding more [redacted] or other non-Trade depths. The [redacted] success of November 1944, in finding depth by using the Hypothetical Additive Bank, had made this approach the primary method for depth finding. By August 1945, this method produced the first of the Canberra (Australia) KGB matches—ultimately an important depth.

Miss Jean Norris—a transfer from the weather section—joined Cecil Phillips, who had now taken full responsibility for machine liaison from Miss Dunning. They expanded the Hypothetical Additive Bank and began machine attacks on other problems. Phillips also picked up responsibility for [redacted] (GRU–naval) and [redacted] (GRU) during 1945. In August 1945, an attack was made on [redacted] (consular) without much success, though Dr Richard Leibler later built on it in the early 1950s and produced some text in conjunction with Meredith Gardner. The [redacted] effort involved isologs, generally circular messages in the same code using different additive pads.[34]

By the end of 1945, Arlington Hall had made an entry into a Russian machine cipher, known as [redacted] or Pink. Senior cryptanalysts Robert Ferner and Mary Jo Dunning collaborated to solve a bust in this system that had been found by Miss Doris Valley (a Cherokee from Oklahoma who was working in the traffic section logging and formatting [redacted] messages). This and some other potential breakthroughs against Russian military systems probably made the Russian Diplomatic problem—Venona—less interesting to Arlington Hall and its consumers, one of the many factors in the slow road to the Venona opening.

H. TICOM and BOURBON: US–UK Joint activities in 1945

Shortly before the end of World War II, the U.S. and the UK began to share the fact of and some details of their Russian Sigint programs and began planning for joint or complementary operations against that target. The codename for the overall Russian target became Rattan and later Bourbon.

The TICOM program (Target Intelligence Committee), established before Rattan/Bourbon, had as its objective the collection of German (and later Japanese) Sigint and Comsec information, records and equipment. It might be compared to the TAREX programs of later years. The TICOM teams found information about Russian systems in the German records and began sending this back to their respective Sigint centers, though with the understanding that GC&CS would be the central repository—actually Arlington Hall, Navy and GC&CS got a copy of everything.

In this section we will trace these two developments. At this stage it is still not possible, or at least not wise from an historical perspective, to completely separate the Venona project from the rest of the Russian program(s). At Arlington Hall, Captain Bill Smith's Russian unit still handled all Russian traffic—Dip, military and plaintext. As we have seen, the entire Russian program was compartmented.

TICOM, with its antecedents and descendants, is a very complicated subject, not least because the records [redacted] are difficult to use. Furthermore, the legends about the OSS and "the Russian codebook(s)" lead to considerable misunderstanding about our Venona breakthrough. It is probably useful to give the most important conclusions in advance, expanding on them in this and later sections as necessary. These conclusions:

1. The people who broke the KGB and GRU systems—Venona—have no recollection of seeing, hearing about, or using any Russian cryptographic material provided by the OSS. Meredith Gardner and Frank Rowlett

[34] Ibid.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

were quite plain-spoken on this point. Likewise, Ferdinand Coudert, at the center of the Russian program before the Venona break (Spring 1943 til the end of 1945) said the Russian unit received nothing of interest from the OSS. The documentary evidence supports this.

2. The TICOM operation, conducted by US–UK military and naval personnel from the cryptologic and intelligence services, did acquire Russian cryptographic material of some importance to the Venona effort. But while that material assisted Meredith Gardner et al in bookbreaking, nothing could be done until the cipher (that is, the additive or key) had been stripped off the message groups to reveal true code groups. At that point, a codebook would be helpful. But, the greatest and earliest Venona break, into KGB system [redacted] was made without the benefit of any captured material that directly concerned that system. It was an immense analytic job involving dozens of people.

3. In the end, the TICOM effort assisted in the US–UK attack against Russian targets and was especially useful for its contribution to a general understanding of Russian systems, and, starting in 1953–54, for the entry into KGB system [redacted] (which had been in use before the [redacted] mentioned above).

September 1944 was a very busy month in the history of special support to Sigint operations against the Russian target —or we should say, potentially important. On 21 September, an advance party of the Finnish Sigint service arrived in Sweden with their records and equipment, an evacuation that had been coordinated with the Swedish services. Within a few days, U.S. State Department representatives began meeting with the Finns to learn about their attacks on U.S. crypto systems (in November, Lieutenant Paavo Carlson of Arlington Hall and Paul E. Goldsberry, a cryptographic officer from State, entered Sweden under diplomatic cover to continue debriefing the Finnish intelligence personnel). On 26 September the Drafting Subcommittee of the just formed Target Intelligence Committee (TICOM) held its first meeting.

As we have seen from the foreign cryptographic intelligence reported in Japanese Military Attache (JMA) communications, the Finns had an active Sigint operation. It had become clear from our reading of JMA that the Finns had been able to read some Russian and U.S. systems, and that they shared information with the Japanese and the Germans.[35] In the summer of 1944, the Finns realized they were on the wrong side and began negotiations with the Russians to save what they could. The Finnish intelligence services did not intend to stay around while the Russians installed a puppet government or occupied the country. The Finns had cooperated with the intelligence services of their neutral neighbor, Sweden, for many years. Major General Carl Ehrensvard, chief of the Swedish Defense Staff worked out an arrangement with Colonel Hallamaa of the Finnish intelligence services for the reception of Finnish personnel, along with their records and equipment. The first evacuees arrived in Sweden on 21 September. The Finns then assisted the Swedes in collection against both Germany and Russia.[36]

Eventually the Finnish Sigint group and its records, memories and equipment would be known as source Stella Polaris, and by the British, who later had some control over them, as Source 267. In some ways Stella Polaris/Source 267 and TICOM drew from the same fundamental source for information on, at least, Russian Dip, including KGB and GRU. It came about something like this. The Finns (presumably their security police)

[35] Finland, perhaps because it had paid its World War I debt to the U.S. and had waged a very heroic fight against the invading Russians in the war of 1939–40 (the Winter War), enjoyed a good reputation with the U.S. and UK. Colonel John Tiltman of GC&CS had established Sigint liaison with the Finns in 1940. But in order to recover lost territory, Finland made a secret alliance with Nazi Germany in 1941, and then joined the Germans in the invasion of Russia. Finland also allied itself with Japan becoming a partner in the Axis combination.

[36] [redacted]

(b)(3)-P.L. 86-36

(b) (1)
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

had entered the Soviet consulate at Petsamo (Pechengo), Finland on or about 22 June 1941, when the Germans began their invasion of Russia. The Finns didn't join the invasion forces for several days but apparently the Russians went to emergency destruction and evacuation procedures right away. It is also possible that German forces (from the occupation forces in Norway) actually got into the consulate, as Germans staged through the Petsamo area. In any event the Russian destruction procedures were incomplete and the Finns grabbed what turned out to be a partially burned codebook of the First Chief Directorate of the KGB, that is the foreign intelligence element of the organization responsible for espionage and counterespionage abroad. This codebook (KOD POBJEDA), and its indicator system later came to be known as [redacted] The Petsamo trove also included KOD 26, a true Dip (consular) codebook, and at least one GRU codebook, as well as rules for using the one-time pads (the additive) to encipher groups from the codebooks, and instructions for using an emergency cipher system in case of compromise of the regular systems. The latter, known in the Venona world as the "Petsamo Emergency System", gave US–UK cryptanalysts an idea of how the Russians used these special hand systems, so important to agent operations.[37] Some traffic, plaintext and cipher text was also taken at Petsamo. Another important find, KOD 14, used by the NKVD rear service security troops, had been seized by the Finns during military operations on the Karelian front.

So, the Finns made a substantial haul at Petsamo and elsewhere. Photocopies went to the Germans, and probably the Japanese. The Swedes got their copies in 1944. This material formed an important asset of the Stella Polaris/Source 267 group. When the British took over this source in 1946, they too got copies of the Petsamo material and passed more copies along to the Arlington Hall. During 1946, the OSS successor/CIA predecessor organization, which (as the OSS) had infiltrated the Stella Polaris group starting in 1944 or 1945, also got some of this material. However, the real story is this: in 1945, TICOM had already obtained all of this and more in their sweep through the German Sigint centers, the teams seizing German photocopies of the material originally taken by the Finns (or maybe the Germans themselves) at Petsamo.

On 29 Sep 1944, L. Randolph Higgs of the US Embassy in Stockholm secretly met with the Finnish Colonel Hallamaa to learn about the apparent exploitability of our codes and ciphers, especially State Department systems. In a memorandum concerning that meeting Higgs wrote that, "(we) were most careful at all times to say nothing regarding any similar activities on the part of the United States, or to give away any information regarding our codes which Col. Hallamaa did not demonstrate beyond all doubt he already had." The Finn certainly gave Mr. Higgs an earful, and Higgs reported:[38]

> *They [the Finns] had been greatly aided in their work on breaking our strips by carelessness on our part in the preparation of messages; (for example) we were constantly putting information in ciphers they had already broken regarding messages in new ciphers, after which they could 'crack' the new ones.*
>
> *His general confidence in their ability to decode any of our messages anytime they wanted to, suggests very strongly that they do just that.*

[37] These systems might be based on a book or statistical chart or a remembered phrase. The agent and the Center would have the same edition of the book (perhaps a novel or travel book) and could construct keys and encipherment tables from them. Many Venona messages talk about systems of this sort, sometimes naming the book that agents in Mexico and South America will use in secret- writing letters or clandestine radio communications. The Petsamo Emergency System was for the consul, but the crypto procedure was the same for the KGB (who after all designed all crypto systems for all users).

[38] The Higgs memorandum, dated 30 September 1944 is in the CCH Collection. Hank Schorreck, Agency historian obtained a copy at the National Archives.

Most of their efforts, he pointed out, were naturally exerted on Soviet codes, of which he claimed they had broken over a thousand. He exhibited convincing specimens of their work on Soviet codes.

One day in early November Colonel Harold Hayes, chief of Sigint operations at Arlington Hall, told Lt. Paavo Carlson (whose earlier personnel recruiting duties are described in Chapter II) to immediately report to the Pentagon for a meeting with Carter W. Clarke. At that time Carlson was working on the Finnish problem [redacted] for Mr. Arnold Dumey. Colonel Clarke told him he would be going to Stockholm to act as an interpreter. Clarke said that he would be met there by Colonel Raines, the U.S. Military Attache to Sweden and his assistant, Major Robert Wood, but Carlson was not to show that he already knew both of them. By coincidence, he had worked for them when they were, respectively, the G–2 and assistant G–2 at First Army Headquarters, Governor's Island.[39] Clarke then sent him to the State Department where he was given a new background identity, as a State Department employee who had graduated from the University of Alabama (rather than his actual school, Clemson). He retained his true name, however.[40]

The next day Carlson and State Department cryptographic expert Paul E. Goldsberry flew out of Andrews AFB, eventually reaching Stockholm after layovers in Iceland and Prestwick, where Count Bernadotte joined the flight.

Starting on 16 November 1944, Lt. Carlson and Paul E. Goldsberry began questioning Finnish Sigint personnel. In commenting on their report dated 23 November, Mr. Higgs of the U.S. Embassy made this important remark (he had been at the sessions too):

At no time did we receive any Russian code material nor did we ask for any from the Finns.

The Carlson/Goldsberry report, which bears no letterhead or subject line (and no signatures, only initials) described in some detail how the Finns had exploited U.S. Dip systems and that they and the Germans were exploiting many other Allied and Neutral systems too. The Finns denied that they had given anything to the Japanese! Carlson and Goldsberry summarized some of the comments the Finns made about their work on Russian systems:

Russian diplomatic codes are unbreakable—said they used a block of cipher groups and enciphered plain text only once on each group.

Captain Palle [a Finnish officer] stated that collaboration with Germany consisted of exchange of information regarding Russia. Just enough to be an ally. Stated you have to 'give a little and take a little'.

Entire (Finnish) organization 1000–1200 people of which greater part worked on Russian military and naval codes with such success that they were able to break a new code within two weeks after its first appearance.

---

[39] Major Wood, a West Point graduate, was the son of General Robert Wood, the CEO of Sears, Roebuck. He had left the Army during the Depression to free up a Regular officer slot for the Army, which was then going through a reduction. Colonel Al McCormack was presumably referring to Colonel Raines when he mentioned having told the G–2 at Governor's Island (Ft. Jay) about the Coudert Commission records concerning communist activities in New York. Ferdinand Coudert, of the [redacted] problem was the brother of that (then state senator and later U.S. representative) Coudert.

[40] Clemson was an all male military college at that time—perhaps the University of Alabama gave better civilian cover while yet being a Southern school. Carlson had been commissioned through ROTC at Clemson. He was working as an insurance agent in New York City when called to active duty in June 1941. Carlson had been born in the Finnish neighborhood of New York City and spoke the language.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

> *He broached the subject of some of their experts going to the United States where their analytical ability could be put to use.*[41]

Interestingly enough, Paavo Carlson's most vivid memory of these meetings concerned German, not Russian, material. He recalled how OSS officer Wilho Tikander opened a suitcase filled with U.S. currency and handed it over to the Finns, in exchange for a German Enigma machine with the wheels.[42]

The Stella Polaris (Finnish) group continued to make overtures to the British and Americans during the last year of the war, eventually becoming, as stated, the British Source 267 re-located to Paris. Apparently they did indeed, as the legend has it, sell Russian codebooks to the OSS.[43] In January 1945, the Swedes returned to the Russian controlled government of Finland some of the material that had been brought out by the Finnish Sigint Service. Nothing of import was returned, unless it had first been copied. The OSS view of the Stella Polaris group was that:

> *On the basis of the record and of inside information which indicated more or less complete penetration of the Finnish resistance—and of Stella Polaris itself—by Soviet and Soviet-controlled Finnish agents, [OSS] rejected these overtures and restricted itself to the counter-espionage coverage and limited positive intelligence exploitation of the group's facilities through our own agents within it.*[44]

In a memo of 11 Oct 1946, the Army G–2 gave the Director of Central Intelligence an appraisal of the Stella Polaris/Source 267 material and some background, concluding that most of the material had already become available through TICOM—but that it was well to keep this emigre Finnish Sigint group occupied lest they sell out to another party.[45]

One final note on the OSS and Russian material. We know that General William Donovan, chief of the OSS, with the approval of President Roosevelt, entered into negotiations and an exchange agreement with the KGB concerning operations against Nazi Germany. According to General Deane, the head of the U.S. military mission to Moscow, who acted as Donovan's liaison to the KGB, the OSS gave the Russians a considerable amount of information (and of course got little in return) including some documentary proof that the Germans had broken certain Russian codes (which seems to be a separate episode from the November 1944 purchases

---

[41] Hank Schorreck also obtained a copy of this memo from the National Archives.

[42] In our interview, Mr. Carlson had no recollection of the discussion with the Finns about Russian cryptography. He believed that the sessions he attended were unilateral—that is the Swedish services were not present. Tikander and Colonel Raines seemed to be in charge. Carlson noted, however, that he was under surveillance and his hotel room searched, presumably by the Swedish security police. (However, he did identify his initials on the aforementioned report).

[43] See The Shadow Warriors, by Bradley F. Smith (Basic Books, New York, 1983). I have not looked at Smith's sources or otherwise examined OSS records (other than those held by NSA). Briefly, Smith's story is this: "In November 1944, OSS Stockholm was offered an opportunity to buy from Finnish sources numerous Soviet military documents . . . in early December, OSS Stockholm purchased 1500 pages of Soviet material and the code keys from Finnish representatives." And, "On 11 December, Donovan reported to Roosevelt that he had purchased one military and three diplomatic codes and turned them over to the State and War Departments." This cryptographic material was ultimately returned to the Russians on orders of Secretary of State Stettinius. We will discuss some of this again in the chapter on KGB/GRU penetration of the OSS. We have, of course, no record of any Russian material acquired by the OSS ever reaching the War Department.

[44] Memorandum for the Director of Intelligence, the Pentagon (i.e., G–2) from the Central Intelligence Group, 4 November 1946. NSA Archives CBRJ 23 [redacted] The CIG followed OSS and would soon become the CIA.

[45] Ibid.

(b) (3)-P.L. 86-36

in Stockholm for which see footnote 40). This affair remains murky even today, and we cannot be certain just what crypt material Donovan showed the KGB.[46]

The TICOM came into existence under the auspices of the Chiefs of Staff of the US and UK. Mr. F.H. (later Professor) Hinsley of GC&CS often chaired meetings of the committee.[47] Colonel George Bicher, an Arlington Hall veteran, and General Eisenhower's senior Sigint officer in the European Theater, was the senior U.S. representative. The purpose of TICOM, as mentioned earlier, was the recovery and study of German Sigint and cryptographic materials—to seize important records and equipment, destroy what could not be taken, destroy German Sigint capability, detain and interrogate key German cryptologic personnel. To do all this, the US and UK formed TICOM teams composed of military and naval intelligence people who were to receive support from local commanders. Some of the early plans of the committee now seem a bit fanciful, for example, the plan to use five U.S. Army infantry battalions to seize German cryptologic centers in Berlin.

Eventually, some six joint TICOM teams were established. The team composition, and team numbers changed from time to time, which occasionally makes it difficult to sort out who was doing what. Some well known NSA people were on those teams, including (with their 1944/45 ranks): Lt. Oliver Kirby, Lt. Arthur J. Levenson, T/3 Arthur Lewis, Lt. James K. Lively, Lt. Selmer Norland, T/Sgt George Vergine and Lt.Col. Paul E. Neff; also Major William P. Bundy of that family famous in higher government circles.

Team 3, previously known as Team 5, under the command of Lt. Col Paul Neff, assisted by Lt. Col. Geoffrey H. Evans, Intelligence Corps, British Army, found the Russian material of greatest interest to the Venona story. Other members of that team included Major Bundy, Captain Duncan McIntyre, Major R.W. Adams, Sergeants F.A. Marx, and I. Loram, and Cpl. Schnabel, all of the U.S. Army (all ETOUSA Sigint people). Major Caddick acted as a courier and Lt. Stribling coordinated transportation. Some others probably were on the team.[48]

---

[46] See Deane's Strange Alliance. Deane gives an extraordinary and vivid account of his and Donovan's meetings in Moscow with General Fitin, head of the First Chief Directorate of the KGB (the foreign intelligence directorate). Fitin, covername Viktor, directed the KGB operations against the U.S. One of Fitin's many agents inside the OSS was Major Duncan Lee, Donovan's executive assistant.

[47] Professor Hinsley is principal author of the multi-volume Official History of British Intelligence during the Second World War.

[48] See TICOM/I.1, Final Report of TICOM TEAM 3, 8 June 1945. Lt Col Evans, British Army, probably wrote the report. Mr. Lou Maddison, GCHQ archivist and Venona expert, often cited in this study, told me that Team 3 made the big Russian finds. Happily, Lou gave me an extra copy of this report, because I have not been able to find a copy in NSA records.

LtCol Paul Neff receives the Legion of Merit, July 1945. He headed TICOM Team 3 in the Burg Operation.

Major William P. Bundy, member of TICOM Team 3.

On about 18 April 1945, Lt. Alfred G. Fenn, Provisional Detachment 14, Provisional Government element, First U.S. Army, visited the castle at Burgscheidungen, hereafter Burg, near Naumberg, Saxony–Anhalt in east-central Germany, an area that was about to be turned over to the Russians according to the agreement on Allied zones (the war continued for about 2 weeks after this date). He spoke to the owner of the castle, with Miss Friedrichs and Mr. Rohrbach of the German Foreign Office present to assist in the conversations. Friedrichs, was reluctant to discuss the official duties that she had been carrying out at the castle. Lt. Fenn

returned a few days later to demand more information and learned that Friedrichs and Rohrbach had been with a cryptologic unit of the German Foreign Office working at the castle. Fenn obtained basic information about their work and the records, and then warned them that they would be executed if the files were disturbed prior to U.S. inspection. Lt. Fenn's information about Burg reached Colonel Cleaves, Signal Officer V Corps. Cleaves telephoned Colonel Bicher. A guard detachment from the 102nd Cavalry Regiment then secured the castle.

TICOM Team 3 left Paris in automobiles on 25 April, driving to Burg via Verdun, Wiesbaden, Weimar and Naumburg, reaching the castle on 27 April. They found that Burg had been a principal cryptanalytic center for the Sigint element of the German Foreign Office, with records intact and key personnel waiting around to be questioned—undoubtedly relieved that the Americans and British had gotten there before the Russians. The team worked at the castle and nearby Sigint-related facilities for two weeks, inventorying the material, packing it and questioning the Germans. Security was particularly important, because the Russians were expected to arrive soon. Lt Col Neff arranged the evacuation, to Marburg in the American zone, of all Germans who might have been in contact with the team in the Burg area. Equipment, records and people were flown out of a nearby airfield on 7 May, on 9 May a truck convoy took out the rest of the people and material. On VE Day (8 May) engineers from the U.S. 104th Infantry Division blew up the German machine processing equipment.

The Neff/Evans team shipped the contents of 73 steel file cabinets. The Burg cache included 300,000 pages of material. Major John Seaman, Arlington Hall's chief representative to GC&CS, advised headquarters that the haul included "some 'Bill Smith' material". Smith was at that time still heading the Russian problem.[49] Some of the team's material, shipped to GC&CS for study, was microfilmed and sent on to Arlington Hall rather quickly. In one of the messages concerning the Burg material we read, "Seaman is sending much 'Bill Smith' material"; in another message Smith asks Seaman to microfilm material of interest to him, and in a 25 June report we learn that Arlington Hall had received "further material for Bill Smith", probably picked up by Oliver Kirby two weeks earlier.[50]

[49] TICOMMA Report, 11 June 1945 in the NSA Archives, CBQK 76 in a folder of TICOMMA reports for 1945 and 1946 (TICOMMA meant TICOM Admin reports?)
[50] See the aforementioned TICOMMA folder.

Army Sigint officers in UK, 1943. Oliver Kirby (5th from right), Bill Bundy (far right) and Arthur Levenson (5th from left).

On 10 June 1945, Lt. Oliver Kirby, a U.S. Army Sigint officer, temporarily serving with British Naval Intelligence detachment 12 A/TICOM Team 6, discovered more Russian cryptographic material.[51] Kirby had been commissioned through ROTC upon his graduation from the University of Illinois.[52] In 1943 he went to the UK as part of the 6813th Signal Security Detachment (Provisional), an Arlington Hall field operating unit that had been formed to give the U.S. a greater role in working German Enigma traffic.[53] Most Army personnel detailed to the TICOM teams came from that unit. One of Kirby's TICOM assignments was to interrogate a Dr. Roeder who had been a member of the German Foreign Office Cryptanalytic organization that Lt. Colonel Neff's team had exploited. Roeder was being held at Schloss Glucksberg in Schleswig, near the old Danish town of Flensburg. Mr. Kirby has preserved his notes from that meeting (which he made on the back of a poem written by a British officer):

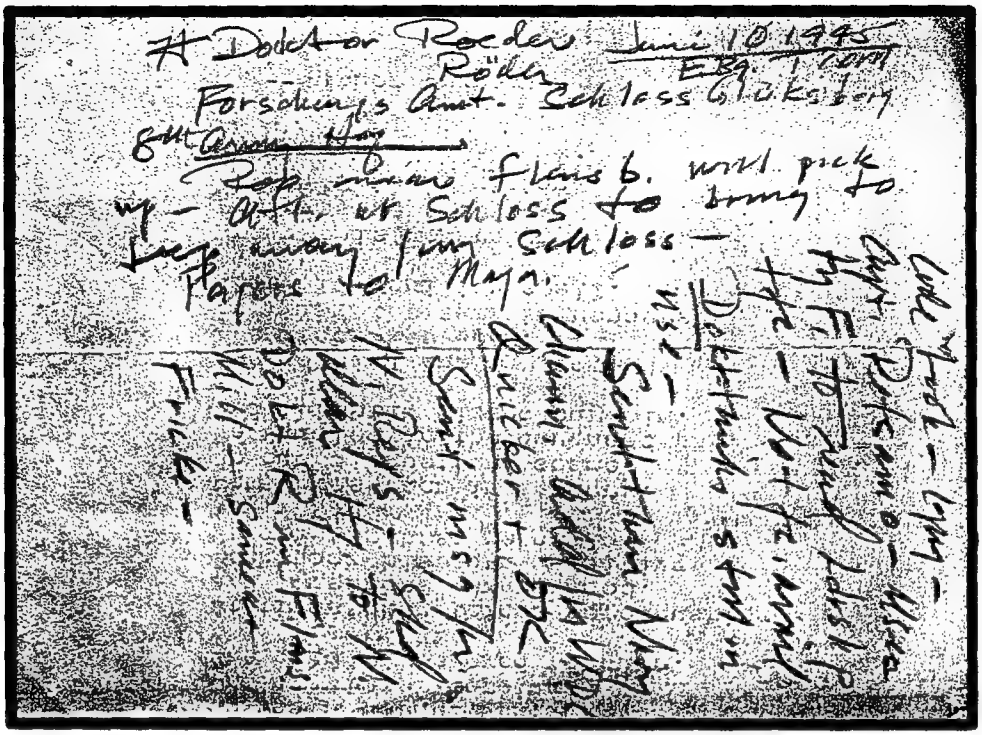
---

[51] Commander Alexander M.S. Mackenzie, R.N.V.R., headed Team 6. Information in this section from interview of Oliver Kirby, in Dallas, Texas, 1 March 1993.

[52] Most of the officers arriving at Arlington Hall in 1942 were reservists who had been commissioned through ROTC. A number of officers, e.g. Ferdinand Coudert received commissions direct from civilian life. By 1943 the Signal Corps Officer Candidate School (OCS) provided most officers for the Signal Security Agency. Very few regular officers served at Arlington Hall or at its field locations.

[53] The organizational history of Army Sigint in the European Theater is most complex. Colonel George Bicher, an Arlington Hall veteran, was the senior cryptologic officer in the European Theater of Operations from 1942–1945. He commanded the Signal Intelligence Division, European Theater of Operations, U.S. Army (SID ETOUSA), with headquarters at 59 Weymouth Street in London. SID–ETOUSA was at once a staff, operational, technical and training organization. It had a field processing element with extensive communications links within the UK, to Arlington Hall and to the Sigint units that went into France in June 1944. Various tactical intercept companies, until deployed to the continent, came under SID–ETOUSA. The 6913th, aimed against higher echelon German communications, also came under Colonel Bicher, as did the U.S. TICOM personnel. The 6913th was housed at Little Brick Hill, near Bletchley Park.

III. THE BILL SMITH ERA NOV. 1943–1946



Oliver Kirby's notes upon recovering Russian Dip codecook, near Flensburg, 10 June 1945.

H. Doktor Roeder Juni 10 1945
Near Flesb., will pick up . . . At Schloss, to bring away from Schloss. Papers to Major.
Code Book - copy - captured Petsamo. Used by [Germans] to read Ldrshp tfc. No tfc. avail. Dokt. thinks still in use.
Sent thru Navy channels. Add. for WDC. Quicker and OK. Sent msg. for N. Reps. Dokt. R. in Flns. Mill—same as Fricke.

Kirby had found a photocopy of Code 26, the Russian consular codebook taken at Petsamo in 1941. Note Dr. Roeder's claim that the Germans read this diplomatic system. This seems unlikely unless the Germans had key pads or had successfully worked Code 26 material enciphered in other than one time pad (such as the Emergency System). Kirby put the material in approved Navy channels and it was flown back to the U.S., probably via London.[54]

In later reports from Major Seaman and his successor Captain C.P. Collins we see the TICOM inventory numbers that had been assigned to the material and can therefore identify items that were later used for the Venona exploitation, T–1014 and T–1015 were, respectively, the GRU (naval) codebook and the KGB codebook for system [redacted]. Seaman describes these as "System TB Petsamo 1941" material and as

[54] Lt. Kirby had other special missions during that time. In one, he and a Royal Marine driver who spoke some Russian crossed into the Russian lines at Minden, under a suitable pretext, to look for German atomic energy records that reportedly had been thrown down a well. In a second mission he went to Flensburg to look for a German who had been involved in burst communications. As he drove up to the meeting place at the harbor, a group of naval mines broke loose from storage racks, collided and exploded causing many casualties. He was blown from his jeep and did not meet the burst expert until 20 years later at a conference with the Third Party. He did however track down the designer of the Goliath VLF U–boat communications system—in a field near Kiel where the man was cutting peat. Kirby told me that the Royal Marines' Amphibious Assault Unit (AAU) supported him in all these activities.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

"charred fragments of Russian 4/F Dipl codebook".[55] He and Collins also mention the filming of T–961 and T–3355 (actually identical items) which were later identified as KOD 14, used by the NKVD rear area troops, and TICOM 1 to 7, 9–11 and 14. TICOM 10, apparently included in the foregoing was KOD 26, the consular code only partially burned in the evacuation of Petsamo.[56]

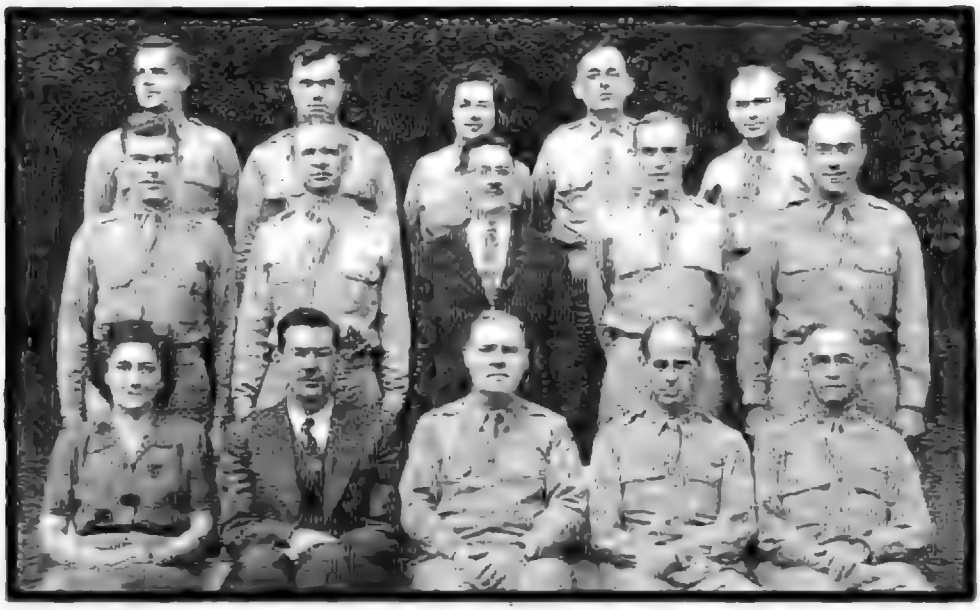
It is this material, mostly recovered by TICOM Team 3, and by Lt. Kirby, that has been the basis for many Venona legends, such as that the breakthrough came about because of a charred Russian codebook recovered from the battlefield, by the OSS or by the Finns and given or sold to the OSS and etc.[57] Some of the material is charred and the circumstances of the recovery are indeed interesting, but for battlefield we have to substitute a classified trash fire at the Soviet Consulate in Petsamo and a collection at a castle in eastern Germany, and for OSS read TICOM Team 3, Oliver Kirby (and the Finns, Stella Polaris/Source 267). Meredith Gardner, who was the first person to recognize the KGB nature of [redacted] later told Bob Lamphere of the FBI that the codebook that he (Gardner) used to make the breakthrough had been found on a battlefield and had a bullethole in it. Meredith later told me that he was referring to a mark that looked like a bullethole but certainly wasn't. We are getting ahead of the story, but the book that Meredith was using was the aforementioned KOD 14, which he studied to learn possible KGB codebook vocabulary and just to see what a Russian codebook looked like. It was not a Venona system, and did not lead to the first Venona break, which was accomplished by bookbreaking without the benefit of the relevant book [redacted] Pages 86 and 87 of the KOD 14 book (which I've only seen in photocopy) do indeed show a round, but irregular, black mark—probably an ink blot.

Soon after the TICOM teams had been deployed to the field, the U.S. and UK made arrangements to cooperate on the Russian problem. The U.S. used this development to further the process of Army–Navy Sigint consolidation that finally led to the creation of AFSA and then NSA. In July 1945, Captain Joseph Wenger of OP–20–G and General Preston Corderman, head of the Arlington Hall operation (soon to change its organizational name from Signal Security Agency, SSA to the Army Security Agency, ASA) agreed that liaison with the British on Rattan, the codename for the Russian problem, would be under the auspices of the joint Army–Navy Communications Intelligence Coordinating Committee (ANCICC) rather than individually be each service.[58]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[55] Memo Seaman to CG SSA, 17 July 1945 in NSA Archives, CBQK 47.
[56] The Seaman and Collins reports are in the NSA Archives at Ibid.
[57] The Final Report of TICOM Team 3 does not specify what documents were found at Burg. Mr. Lou Maddison, GCHQ archivist, told me that Team 3 made the major finds, including a copy of KOD PODJEDA and the other Petsamo items.
[58] Memo Wenger to OP–20, 16 July 1945. NSA Archives at CBQM36 in folders "Bourbon Semi-Monthly Reports and Related Documents". Except as otherwise noted, my brief summary of Bourbon is based on that collection of papers and no further citation will be made. Both the NSA Archives and the CCH Collection have other groups of documents on this subject.

III. THE BILL SMITH ERA NOV. 1943–1946



LtCol Frank Rowlett with staff, 1945. Bill Smith (top row, 2nd from right) and Maurice Klein (far right 2nd row).

British and American cooperation on the Russian problem developed very quickly as outlined below in a series of quotes and extracts from ANCICC (later called STANCICC, with State Department added to Army and Navy) Bourbon progress reports. One interesting US–UK policy item, before we catalog the Bourbon evolution: it became apparent early on that the U.S. would no longer conceal from the British its work on Russian Dip and would willingly share not only "fact of" but also technical details. Edward Christopher and later Cecil Phillips would be sent to the UK to further this process. But once Arlington Hall discovered what was in the traffic—that it was not Dip but espionage traffic—a U.S. eyes-only policy would again be imposed, though briefly and probably not very effectively. A story for later sections of this study.

The Bourbon highlights:

- 7 Aug 1945. Major Seaman authorized to open negotiations with the British — first step to negotiate for immediate complete exchange of traffic, status of solutions, technical materials, techniques. Seaman to suggest to British that the codeword Bourbon replace Rattan.

- Seaman had learned on 5 Aug that British had only 3 or 4 months worth of Russian Dip traffic; no cable traffic to/from London but collection would begin.

- 8 Aug 1945. Washington to send Major Seaman additional information on Russian Dip systems with proposal that US–UK exchange back traffic on microfilm.

- 15 Aug 1945. Arlington Hall and Navy have identified 35 Russian systems, of these 6 were Dip and 2 of these in process of solution: depth of overlaps limited to two. TICOM has made clear that Russians use one time pads to encipher codes. Other than Dip, all US intercept from Russian Far Eastern nets.

- 15 Aug 1945. Sir Edward Travis, head of GCHQ "has confirmed our proposal that cooperation on Bourbon is to be complete, though informal". Travis has given Major Seaman access to all UK Bourbon material.

- Sep 1945. Discussion of further exchange of liaison officers.
- 16 Oct 1945. US liaison officers touring all British field stations.
- 16 Nov 1945. Captain C.P. Collins to relieve Major Seaman and Mr. Ed Christopher to relieve Mr Frank Lewis for Bourbon liaison at GCHQ.
- 1 Jan 1946. Arrangements for exchanging all Bourbon translations including back material.
- 16 Mar 1946. US begins receiving films of Source 267 material.
- Throughout this period, much discussion of Russian machine ciphers (military/NKVD)
- 27 June 1946. Bourbon liaison has been removed from special category, that is, the general Russian Sigint problem no longer a special compartment — Venona soon would be compartmented.

In the midst of all this, "C" wired the GCHQ representatives in the US as Immediate, 23 Sep 1945:

> *R.C.M.P. have in custody a cypher clerk from office of Soviet Military Attache. He has already provided some useful crypto information.*
>
> *Canadians have agreed, at our request, that he should be interrogated at once by American officer, if Americans will consent. We consider his information will probably be of considerable assistance if he is interrogated on technical matters by an officer fully versed in crypto problem involved.*
>
> *If Americans agree to send an officer (and Canadians ask that it be restricted to one only), please arrange that he contacts Stephenson in New York who will hand him over to appropriate contact in Canada. This is necessary to avoid crossing lines with FBI. Stephenson is steering FBI interrogations in Canada clear of crypto matters.*

A follow-up message the same day gave some crypt intelligence that the defector had provided in preliminary debriefings. The message specified that the point of contact for the U.S. would be Sir William Stephenson, head of British Secret Service operations in the Western Hemisphere 1940–45 (sometimes referred to as "Intrepid").

The ANCICC learned the next day from Group Captain Jones, a GCHQ liaison officer, of the foregoing. "After clearance from 20–G, Cominch, and G–2 was obtained, it was agreed that it might be profitable and not too dangerous to take advantage of the opportunity to have an Army officer interrogate the clerk."[59] Lt. Colonel Frank B. Rowlett departed Washington, in civilian clothes, on 25 September 1945, to question Lt. Igor Gouzenko, the GRU code clerk who had defected. The KGB almost caught Gouzenko, and after he got away KGB officers using crowbars broke into his apartment, but were turned away by the police. As we would later learn in the eventual decryption of one of the most famous Venona messages, Kim Philby had alerted KGB London upon learning of a message from Stephenson to "C" announcing the defection.

I. Gouzenko, Bentley, Chambers and the Anonymous Letter

A stunning series of closely spaced counterintelligence events took place in 1945: on 10 May the FBI had conducted a serious, all-day interrogation of Whittaker Chambers at his Time magazine office (Chambers earlier attempts to tell all had gone astray in the hands of A.A. Berle and Director Hoover); Gouzenko of the GRU defected in September; Elizabeth Bentley, a veteran KGB officer, gave the FBI a 107 page statement in

[59] From the collection of Bourbon papers cited above.

November. And for the past two years the FBI had been studying an anonymous letter, from a KGB (or just possibly GRU) officer. An incredible amount of information became available on Soviet espionage in the United States—but with very little documentation to back it up. Whittaker Chambers had saved a few papers that would help convict Alger Hiss; Gouzenko had a lot of papers on Canadian, but not American spies; Bentley, with the most to tell, had only her recollections. Venona would eventually provide the missing documentation and identify many more spies.

Frank Rowlett spent several days questioning Igor Gouzenko, codenamed "Corby", and the following paragraphs are based on his "Special Report on Bourbon Cryptography: Report on Interrogation of Corby", dated 15 October 1945.[60]

Rowlett learned that Gouzenko had gone to the RCMP o/a 10 Sep 1945, in fear of being called back to the Soviet Union because he had committed a serious security violation. He had first tried to go to Canadian newspapers with his story of Russian espionage but had been turned away (Russian trade official Kravchenko had "defected" to the New York press in 1944, reasoning that by going public he would be protected. We will see in Venona how the KGB and their American agents tried to track him down.) He then tried the Justice Ministry but was again rebuffed. Finally, the RCMP took him into protective custody (along with his pregnant wife and young son).

Rowlett drove to an isolated, lakeside summer cabin some 90 miles from Ottawa where Gouzenko was under guard. The Rowlett party included Professor Gilbert Robinson, a wartime Canadian Sigint officer, Inspector Leopold of the RCMP and a driver. (Robinson had conducted the preliminary questioning of Gouzenko on cryptologic matters— Gouzenko had given names of spies and supporting papers to the Secret Service, RCMP and FBI.) Rowlett learned that Russian cryptography, in the external affairs area, could be divided into two types:

- Systems used by Russian establishments abroad in communication with Moscow. These systems were entirely by encipherment of a code by a one-time additive.
- Emergency or illicit systems which used a substitution alphabet based on one and two-digit equivalents *for the* Cyrillic alphabet, which would then be enciphered by a one-time key generated from a book or other publication readily accessible to both Moscow and the communicant in the field, i.e., both Moscow and the field had to have the same book, same edition.

Gouzenko explained Russian crypto-security doctrine and procedures, and the day to day work of a GRU code clerk. All code clerks were approved and trained by the KGB. Every Russian official authorized to sign messages—the GRU Resident/Military or Naval Attache, the Trade Representative, the Ambassador or Consul had a code clerk assigned to him who would prepare the messages. These clerks were responsible to the KGB for security and procedures—the officials who drafted the messages could not keep file copies of the original texts of the messages they were releasing. In the case of the GRU Resident in Ottawa, he would bring his notes into the office of the code clerk, and in the presence of the code clerk write out a message. The code clerk, after the drafter had left the office, would encode the message and then take it to the mission's communications officer who would give it an external serial number and take it to the commercial cable company for transmission to Moscow (the Russian establishment in Ottawa did not at that time have its own communications facilities).

[60] Copies in the Venona Collection, but also in the NSA Archives at CBQM36.

The Russian text of a GRU message would be encoded by a four-digit, one-part code, that is, the code book was arranged in strict alphabetic order. When an item had to be put in the message for which no equivalent appeared in the code book, it was spelled out by means of a Cyrillic or Roman substitution alphabet which was issued as a supplementary chart to the code. When this chart was to be used the four-digit group 7810 would be entered, meaning "begin spell" and the end of the spelling would use a special two digit group, 91, to mean end of the spelling.

The GRU code text would then be enciphered by a one-time pad. All pads, for every agency of the Soviet government, were manufactured by the KGB. The pads had either 35 or 50 pages each and each page would contain ten lines of five 5–digit groups, for a total of 50 groups or 250 digits per page of pad. Each page or sheet of the pad had a two digit number in the upper left hand corner ranging from 01 to 35 or 50 depending on the number of pages in the pad. These pads were carefully packaged and controlled. When the message reached Moscow, a senior officer would determine the addressee and pass it to the appropriate code clerk. Gouzenko reported, curiously, that copies of these GRU messages would go directly to the KGB for analysis (perhaps he meant, also to the KGB). Gouzenko described for Rowlett, at some length, the emergency or illicit systems.

Gouzenko believed that the KGB, in producing all one time pads for the government, mechanically generated them using an apparatus, "which selects numbers purportedly at random by a device using small balls in some fashion. This apparatus was credited to the British originally, but certain improvements were made by the (KGB) cryptographers when it was adopted by them. No further information regarding pad generation is available."[61]

Rowlett concluded his report with a general observations section:

- While the KGB carefully screened candidates for work in the cryptanalytic organizations, the "standards are not so high as those set for cryptographers".
- A code clerk underwent 9 months of training.
- A code clerk was expected to have familiarity with the language of the country of assignment and be able to evaluate open source publications of that country.
- During the war, the Russians had considered the German one-time pad Dip systems as invulnerable as their own. (note by rlb: late in the war, Arlington Hall broke into the German one-time pad system, which undoubtedly led to optimism about eventual success against Russian Dip too).

A small team in Bill Smith's Russian unit consisting of Mrs. Genevieve Feinstein, Miss Mary Jo Dunning and Mr. Burton Phillips immediately began a study of the Rowlett report in context of the traffic on hand. It is maddening for the non-cryptanalyst to try to understand, but then to realize, that even with such a source as Gouzenko, who brought out plaintext of some of the GRU encrypted messages and explained the system in great and accurate detail, the traffic remained unbreakable. Gouzenko's background information on the Russian systems was certainly very important and helpful—but with it Arlington Hall could not read any traffic and could at best only add some words to book breaking vocabulary of the GRU code book. But the code book would not do anything unless the cipher additive, from the one time pads, could be identified and stripped off to reveal the underlying code groups. Gouzenko had no pads, and if he had it would only have given an opening into the message(s) enciphered by that particular pad. Gouzenko's most enduring contribution to Venona was to put the

[61] Throughout this account I stick very closely to Rowlett's words—putting it all in quotes seemed too tedious and I have done some editing anyway.

cryptanalyst into the office of a Russian code clerk, giving us an understanding of how he worked, and what his systems looked like and how they were used.

Whittaker Chambers and Elizabeth Bentley gave the names of KGB and GRU agents in the U.S., more than a year before the first Venona translation. A quick summary of their information is useful to the story of Venona and its place in U.S. counterintelligence history.

Whittaker Chambers

Chambers, a sometime editor of Time magazine, described a GRU network in Washington in the mid–1930s and reported to the FBI that Alger Hiss and Harry White had been members of the group, passing along classified information to the Russians. By 1945, when the FBI interviewed Chambers in detail, Hiss had become an important State Department official and Harry White an Assistant Secretary of the Treasury. Chambers provided enough documentary evidence to eventually convict Hiss of perjury. White, never charged, was still under investigation by the FBI when he died. Chambers could give no significant information about Russian espionage in the U.S. after about 1938 when he severed his Communist Party connections.

Elizabeth Bentley (left) and Alger Hiss (right) at Congressional hearing.

Elizabeth Bentley, a graduate of Vassar and Columbia with various employments over the years, may also have had a GRU connection during the later 1930s, but seems to have signed on with the KGB in 1940, acting under instructions of Jacob Golos, a KGB agent-officer in New York City and major net controller. Bentley served as courier between Washington and New York and sometime agent handler. She gradually lost interest in the work after Golos, her lover, died in November 1943—but it was two years before she ended all contact with the KGB and went to the FBI. In her long statement to the Bureau, Miss Bentley named almost 100 Americans and Russians connected to espionage or Communist Party activities in the U.S. Of the Americans, 51 were investigated by the FBI (27 of these held U.S. government positions as of the date Bentley went to the FBI). In terms of Venona, Bentley's information undoubtedly helped identify covernames in the traffic; she herself appears in the Venona decrypts seven times under the covername UMNITsA (Good Girl) during 1943 and 1944 and seven more times under the covername MIRNA during 1944—in fact some of the most interesting KGB tradecraft and security policy information in Venona concerns her. She told the FBI that Harry White was working for the KGB, as was Major Duncan Lee, sometime executive officer to General Donovan, head of the OSS. She described the agent net run by Gregory Silvermaster, a government employee, and named the people under his control. As we have seen, she told the FBI that the KGB had learned something about Arlington Hall's Russian Sigint program. Some 29 Americans identified by her as having connections to the KGB appear in the Venona traffic. Undoubtedly many more are in Venona as unidentified or unrecovered covernames. Venona identified more spies, in nets with which she was not involved. We can state quite confidently that the controversial information she provided, first to the FBI and later to a grand jury, to Congress and to the public, was accurate. Unfortunately, most of the information she gave would be insufficient for prosecution. She brought out no papers and no one (almost no one at least) provided any corroboration.

While it is generally believed that the Gouzenko-Chambers-Bentley revelations of 1945, were the first real break into Soviet espionage in North America, one more source needs to be mentioned: the Anonymous Letter of 1943. Written in Russian and addressed to FBI Director Hoover, the unsigned and undated letter was postmarked Washington,D.C., 2 a.m., 7 August 1943. The writer has never been identified but was presumably a KGB (or possibly GRU) officer assigned to Washington. This strange document named only two American agents of the KGB, but identified major officers of the New York, Washington and San Francisco Residencies—once again, names that would figure prominently (under covernames) in Venona.[62] The writer said he was coming forward because KGB officers in the U.S. were in the pay of Japan! This absurd statement may have been made because the author feared his information on Russian espionage in the U.S. would be ignored unless it was somehow connected to the Axis. Some highlights of the letter (which appears in full in an appendix):

- U.S. Communist Party leader Earl Browder was a KGB agent.
- The KGB chief in the U.S. was Vasili Zubilin (true name Zarubin), assisted by his wife, also a KGB officer.
- Zubilin's principal assistants included Pavel Klaren, vice-consul in New York; Khejfets, vice-consul in San Francisco; Kvasnikov, the technical intelligence chief; Shevchenko, operating in Buffalo under Purchasing Commission cover; Mironov (true name Markov) and more.

[62] The Anonymous Letter named Boris Morros of Hollywood and C.P. Chairman Earl Browder as KGB agents.

• Zubilin, a KGB general, had directed NKVD police and troop work in the occupation of eastern Poland in 1939, and with Mironov, had been in charge of the murder of the 10,000 Polish officer prisoners thereafter (the reference here is to the Katyn Massacres of 1940).

All of this information was true and much elaborated upon in Venona, e.g., Khejfets the KGB Resident in San Francisco; Kvasnikov running the atomic bomb espionage operation. We probably see reflections in Venona of the FBI investigation into the leads provided in this letter, for example the KGB in New York and San Francisco reporting to the Center about increased FBI surveillance activities; Zubilin complaining to Moscow that his activities in Poland have apparently become known.[63]

[63] See Appendix Two of this study for the text. Copies of The Anonymous Letter are in the Venona collection in box D046, 54–001 and elsewhere. Arlington Hall seems to have gotten its first copy of this letter in about 1949. Meredith Gardner made a translation of it, that is, he did another version to add to the original FBI translation. Bob Lamphere told me that the Bureau made a tremendous but unsuccessful effort to identify the writer—one can only wonder what would have happened if the writer could have been grabbed and turned (or simply taken in as a defector). This letter is of considerable historical importance and raises many questions about U.S. counterintelligence during the war.

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

Non - Responsive

VI. US–UK PROGRESS 1948–1952

Dame Elizabeth Hill's first Russian language course for British intelligence personnel, Cambridge, 1945–46. Included in photo are some who later worked Venona: Sir Peter Marychurch, Geoffrey Sudbury, Patrick FitzPatrick, Tom Moss, Howard Vincent.

A. ASA–GCHQ Collaboration During 1948 and 1949

In Chapter V., Cecil Phillips described the various components of the cryptanalytic attack on [redacted] during the period 1945–49, though again we note that the Russian Dip problem was attacked as a whole. It happened, however, that the most important part of that Dip, the KGB traffic, proved to be the most exploitable (except for Trade). In this chapter we will resume the chronological history, noting various highlights in policy, collaboration, analysis and counterintelligence. Much of this part of the story is traced through GCHQ and UKLO papers—carbons given to the ASA Russian Dip unit, which are now filed in the NSA Venona Collection. Counterpart ASA/AFSA records, if they ever existed, are not to be found, though the early translations by Meredith Gardner and various FBI studies and reports certainly are a major source of information on end product and counterintelligence.[1]

[1] Stuart Whittle, one of the first persons I interviewed (and this was before looking at any of the Venona Collection), told me not to expect to find extensive policy or CI analytic records at NSA. He was right of course—the people working Venona were very cautious and tended to limit themselves (with significant exceptions) to cryptanalytic papers and translations. In any case, the UK Venona representative at Arlington Hall needed to keep GCHQ informed, especially during the early years when Venona was primarily an ASA/AFSA operation.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VI. US–UK PROGRESS 1948–1952

The natural division of effort on counterintelligence matters between Gardner and Howse was along national lines—Howse and GCHQ to work the Commonwealth lanes and Gardner the New York KGB traffic. But early in 1948, ASA began officially releasing to GCHQ traffic on the New York–Moscow lanes that appeared to relate to the UK.

On 27 February 1948, Howse sent GCHQ all traffic data known to ASA about KGB messages of 1945, 1946 and 1947 on the Canberra <—> Moscow lanes as well as the matching statistics for this traffic (that is the KGB messages that had been matched with other systems and therefore were being or would be decrypted).[2] Howse followed this with a much more detailed report on 31 August 1948, "State of Solution of Canberra [redacted] Traffic". That report contains a good summary of the ASA group in which Howse worked, that is the group at the end of the cryptanalytic cycle that did key recovery and produced the decrypts and translations (see Chapter V). Howse reported that the group then consisted of seven people (himself included) and that Gardner was the only real Russian linguist in the group. Three people were working Canberra and four New York traffic. Gardner, through analysis, was gradually filling in the unseen [redacted] code book. Howse proposed that GCHQ start its own Russian Dip effort:

> *There is no doubt that solution could be expedited by study at [GCHQ]. It would be necessary for ASA to forward all the numerous aids—code phrase books, analyses of stereotypes etc. etc.—and to keep [GCHQ] up to date in addition lists to* [redacted] *codes (the latter not normally being sent as they are made.)*

GCHQ was already receiving information from ASA taken from the New York traffic, though as late as Jan 1950, the official rule was that, "copies of New York messages will only be passed to the GCHQ unit if (a) they involve, or possibly involve, British personnel, or (b) they are of general interest"[3] Some of the earliest ASA dissemination to GCHQ of translations of this type occurred in June 1948, with the approval of Colonel Hayes, chief of ASA. In one KGB message New York —> Moscow, 17 May 1944, covername KARAS was reported to be going to London regarding Yugoslav affairs; Tito's name appeared in the message and Moscow was asked to telegraph to New York the password that KARAS would use when meeting with the London KGB. In a second New York —> Moscow message, 14 June 1944, KARAS's London password and the meeting place were discussed.[4]

At the end of 1948, ASA turned to GCHQ after having exhausted the search in U.S. records for important U.S. or UK diplomatic documents acquired by the KGB in 1944–45 and described in Venona messages as "G" materials. "G" would eventually be understood to be the same person as covername GOMER, GOMMER and HOMER, that is, Donald Maclean, an official of the British Foreign Office. ASA, with the assistance of G–2, had been unsuccessfully searching State Department records for the "G" documents that had reached the KGB Washington during 1945. In a blind internal memo of 17 December 1948 (probably prepared by or for Oliver Kirby), the writer proposed that "a memorandum be handed to Mr. Howse or Mr. Jackson (UK Senior Liaison Officer Washington) with the object of determining whether the British can supply us with the originals of this material." The request to the liaison officer would be in this form:

---

[2] PH.3. in the Venona Collection. The P.H. (for Phillip Howse) Series was one of several series used by the UK representatives in the U.S. for communicating with GCHQ. Most of this material is in the 3337 group/box 18 of the Venona Collection.
[3] P.H. 85, 11 January 1950, Venona Collection.
[4] New York —> Moscow messages external numbers 699 and 847 respectively. As mentioned earlier, KARAS was Anton Ivancic, active on behalf of the KGB in Serbo–Croatian affairs in the U.S. and Europe.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Some material has been found in [redacted] messages from Washington to Moscow of March 1945 which looks like a series of diplomatic reports. Some indications suggest that this material is of British origin. We should like you to explore this possibility on the basis of numbers and dates given in the preamble of each item plus a general characterization of the subject matter where known, as follows. . .[5]

This paper bears a handwritten notation that "This has been ok'd. Mr Howse will prepare a request to be sent to GCHQ."

GCHQ had renewed its own Russian Diplomatic effort (in H5) by March 1949, as described in a letter from Hugh Alexander to SLO Washington. Alexander explained that technical progress would be reported in the GCHQ H5/WB series and intelligence in their HX series. The work would be confined to Canberra <—> Moscow traffic of 1945–48 that matched with Washington <—> Moscow [redacted] of 1943. It would be worked, "by our own party of four", Mr. Root, Miss Arnott, Miss Mason, and Mr. Bodsworth.[6] Mr. Alexander concluded that GCHQ would "need a great deal more experience and man power to be good at a game which you have done superbly well." (The first GCHQ product, in the HX series, was sent to the SLO for passage to Howse "for the U.S. party concerned.").[7] Over the next year the GCHQ Russian Diplomatic party added at least five more people including Russian linguists Howard Vincent, Patrick FitzPatrick and Geoffrey Furniss, and bookbreakers Colonel Murray and Major Hardinge.[8]

As we have seen, Meredith Gardner had been using the NKVD KOD 14, a 1945 TICOM acquisition, to help him understand Russian code book vocabulary and layout—all as an aid for [redacted] bookbreaking. In March 1949, Gardner and Howse took an interest in TICOM 1015, which had a partially burned cover page that showed only the last two letters of the Russian title: ". . . DA". It may have been lost in the voluminous TICOM archives; and in any event its potential importance had not been recognized. As Howse reported to GCHQ, TICOM 1015 was the "badly burnt encode section of a 2-part 4-digit codebook which has every appearance of being (a KGB) code. This code is far closer to the [redacted] codes than any other TICOM, particularly as regards groups for phrases."[9] The most significant phrase was code group 9338, "Personal to Viktor". Other interesting phrases in the book were "Fellowcountryman", later understood to be the KGB term meaning member of the local Communist Party; and the terms for Intelligence Service, agent recruitment and informers. As we have seen in Chapter IV., this would eventually (actually not until December 1953–Feb 1954) be identified as Code POBJEDA, known to the US–UK as code [redacted] the KGB codebook used by the First Chief Directorate from 1939 or earlier until Nov/Dec 1943. Absent matchable traffic, nothing could be done to exploit this system in 1949 and for several years thereafter. But POBJEDA, though half the book had been burned, must have been of some help to Gardner and his associates in filling out the meanings in book [redacted] and getting a better

[5] Memo 17 December 1948, no signature, subject or other heading. Meredith Gardner probably wrote this for Kirby to pass on to Hayes for approval.
[6] H5/WB/001, 25 March 1949 in the Venona Collection, group 3337, Box 18.
[7] See note from GCHQ's AD(P) to SLO Washington, DGC/234 7 March 1949 in collection cited above.
[8] H5/WB/040, 25 April 1950. Apparently there were more than five additional personnel on the Russian Dip target as the qualifier "including" is in this letter.
[9] P.H. 28, 7 March 1949.

~~TOP SECRET UMBRA~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

sense of KGB tradecraft language.[10] During early 1951, Patrick FitzPatrick, at GCHQ, would complete the collation of TICOM 1015 and the Consular KOD 26 [redacted] "the last two were printed by IBM in two parallel columns starting level at the first entry under each letter. Only the code groups and existing values were printed . . . and a wide margin was left on the right of each sheet to allow space for insertion of candidates from the two TICOM documents for the missing meanings."[11]

Some other highlights of 1949 (as described in Howse/GCHQ papers):

• Carter Clarke, now chief of ASA, approved passage of two [redacted] translations direct from Howse (perhaps via the SLO) to Peter Dwyer, the British Secret Service representative in Washington. (P.H.35, 20 April 1949)

• Howse noted to GCHQ that their "approach to the problem is probably a little more systematic than that adopted here at the present time. We (at ASA) rely more on the experience of personnel as to the likely contents of messages rather than on a set of established rules for breaking into them." (P.H.36, 3 May 1949)

• As of April 1949, 4144 true values had been made in 10,000 [redacted] system (about half of the final total for recovery of values—that is, meanings—in this never-seen book). (P.H.41, 9 May 1949)

• Miss Marie Meyer (the first [redacted] bookbreaker in 1945–46) had rejoined the section (P.H.48, 16 June 1949)

• Howse sent GCHQ copies—apparently typed from the original TICOM documents—of KOD 26 (Consular) and the aforementioned 1015, both from the Petsamo trove. (P.H.48)

• ASA had determined that the change from [redacted] took place between 9 January and 4 February 1946. (P.H.54, 7 July 1949)

• Howse also discussed findings on KGB and Trade Cipher Instruction messages (service messages) and gave GCHQ a general rundown on "Encoding Habits in [redacted] Pad Systems"—paragraphs on subjects such as addresses and signatures, text beginnings and endings, continuations, pads for circular messages. (P.H.55, 9 July 1949). Throughout the Venona period, ASA/NSA and GCHQ references to Cipher Instruction messages are abbreviated as CI or C.I., a confusing form considering that Venona concerned counterintelligence, usually called (at least in the U.S.) CI or C.I.

• The first KGB traffic Mexico City —> Moscow (1944) had been matched at Arlington Hall. (P.H.66, 13 September 1949).[12]

---

[10] Meredith Gardner told me that he had originally thought the ". . . . DA" might be the last two letters of the Russian word for fishhook. The KGB defectors, Mr. and Mrs. Petrov, identified the title of this code as POBJEDA, meaning " victory". The GCHQ [redacted] handbook, a learning aid for analysts, helps date the full identification of TICOM 1015/POBJEDA. The second edition of the supplement, "[redacted] Code Check List", dated 25 September 1953 (more that four years after Howse's P.H.28), listed ". . . DA" as TICOM 1015, "German photostat of original. Charred fragments of original" and that it was also carried as TICOM 3582. Neither the check list or the original handbook itself identify it as KGB. However, in a supplement dated 12 Feb 1954, it is correctly identified as: Code [redacted] TICOM 1015 and we learn that "NSA has recently (Dec 1953) made a break into [redacted] in the New York lane. . . . there are no true matches involving this code . . . so far our knowledge of the code has come entirely from the TICOM copy." Sam Chew and Cecil Phillips made the Dec 1953 break, discussed below. POBJEDA had been found by Paul Neff's team in a German castle in Spring 1945, as described earlier.

[11] Letter, A.G. Royffe to Howse, 8 February 1951. Copy in Venona collection.

[12] The Mexico City <—> Moscow traffic is historically important and is covered in a separate section of Chapter VIII.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

~~TOP SECRET UMBRA~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

• Organization and management: Wilma Berryman who had been running the Russian Dip unit to be replaced by Ed Christopher (a veteran of the Russian problem who had been at GCHQ on a liaison assignment at the time Bourbon started). (P.H.66)[13]

• Howse sent GCHQ two messages in the New York —> Moscow lane that listed covername changes the KGB made during 1944 (suggesting that the ASA–GCHQ cooperation was now approaching full sharing of product). (P.H.80, 29 November 1949)

At the end of December 1949, Howse signalled GCHQ that some Moscow <—> London [redacted] (uncategorized, but believed to be KGB) traffic of September 1945 had been matched with some New York KGB traffic, "so far the match involves 12 messages to London and 26 pages of pad"—however it would be difficult to strip off the additive because "both members of the new match are in the same 4-digit code, and all groups are in phase."[14] Howse said that the Moscow <—> London traffic on file was from June 1945 and after and had been collected by the Radio Security Service (RSS). The traffic into London looked in better shape than the outgoing. As for the contents of the [redacted]—which was soon found to be [redacted] (KGB)—only a little had been recovered so far, for example seven messages were addressed to covername BOB and four to covername IGOR.

The small group of exploitable KGB messages, Moscow Center to London KGB, all from a single week in September 1945, would be intensively worked over the years. The centerpiece messages would eventually be found to relate to Kim Philby's urgent report to London KGB that Gouzenko was in the hands of the RCMP (actually the warning message from KGB London to the Center could not be read, but the Center's responses and instructions to London were).

B. "Black Friday"—20 December 1949

This event has become legendary over the years, not among people working the Venona problem of course, but elsewhere in NSA and the Intelligence Community. The story goes that we read Russian Dip up to 20 December 1949, but then the Russians—probably because of what they learned through espionage— changed their system, and we lost it forever. The actual story, from the U.S. perspective, is quickly told.

[redacted]

[13] In the earlier part of this study, organization and placement of the Russian Dip problem received a fair amount of attention. During the Venona years this seems less important. The Venona workforce was quite stable and would became a distinct, compartmented unit within the Russian organization (A Group after the early 1960s). Meredith Gardner was, throughout, a technical expert—he did not run the Dip or Venona effort. However, the program is always associated with his name as it should be.

[14] P.H.88, 27 January 1950. I have not found Howse's message of 24 Dec 1949 which announced that the match had been made. This P.H. provides the details.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

C. Meredith Gardner's Translations of KGB Traffic

Venona translations were frequently re-issued when new recoveries were made or the analysts gained a better understanding of the material (from breaking other messages, from information provided by the FBI etc.). While many of the reissues followed new cryptanalytic successes, others were done for linguistic reasons, that is, simply a re-translation.

The sequence and history of early translations is unclear, and we cannot date with certainty when Meredith Gardner began preparing message by message translations in a uniform format. As we discussed earlier, Gardner's product in 1947 mostly appeared in his series of eleven special reports. But during 1947 and especially 1948, Howse began sending GCHQ some of Gardner's product, especially the Canberra <—> Moscow material. He put partial translations and extracts in memos to GCHQ as there were no formally published individual message translations.

Gardner felt hindered by not having a regular customer until Bob Lamphere of the FBI became involved. He was also inhibited by shifting rules on how much he could share, even within the Russian unit. He recalls instructions to withhold the results of his work from not only the Navy, CIA and GCHQ, but also from the people working to support him (see Chapter V for a discussion of the overall cryptanalytic process). Sometime later, perhaps in 1950–51, Katurah McDonald, one of the earliest analysts on Russian Dip, told him how disappointed she was not to have been let in on the core secret—that Gardner was reading KGB traffic. Hers was not an unusual complaint.

A very rough idea of Gardner's production of Venona translations can be had by studying two groups of his early translations.[16] (the earliest groups that have been found, though there are some earlier individual pieces, e.g. the atomic bomb scientist translation). Following is a count of translations in these two collections:

[16] There are a very few earlier individual translations, e.g the atomic bomb scientist message.

I. Vol 1 and 2 of the Collection Labelled: "MKG Translations"

Translations bearing a typed or handwritten date:

1950—35 translations

1951—48

1952— 7

Translations dated by the Comint Codeword then in use, but not bearing a specific date of translation:

1 Sep 1947–1 July 1949	1 translation
1 Jul 1949–1 Aug 1950	111
1 Aug 1950–1 July 1951	61
1 Jul 1951–1 July 1952	28

Grand total of translations 1947–1 July 1952= 291

II. The XY Folder of Gardner's Translations

Translations bearing a typed or handwritten date:

1950— 23

1951— 46

1952— 60

1953— 13

Translations dated by the Comint Codeword, but not having a specific date of translation:

15 March 1946–1 Sep 1947	21 translations
1 Sept 1947–1 July 1949	1
1 July 1949–1 Aug 1950	55
1 Aug 1950–1 July 1951	54
1 July 1951–1 Jul 1952	54
1 July 1952–1 Oct 1953	62

Grand total of translations 1946–1 Oct 1953 = 389.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Note that I. and II. above are separate counts of the same material, that is, they are not to added together.

The translations in group I are all NY —> M KGB; in group II a few Consular [redacted] and KGB Moscow <—> San Francisco, Washington and non-U.S. cities are included. The progress of Gardner's translations could be tracked several other ways, but this will have to suffice.[17] However, we should note a few peculiarities in this dating scheme. For example, some of the translations that I attribute to March 1946–September 1947 (group II) are typed on the back of the pre-printed ASA form containing the Comint codeword of the time (CREAM), which suggests that Gardner was using it as scratch paper. His typed translations, on the blank side of these forms bear no codeword. Therefore, I think it might be well to move some of those 21 translations of March 1946–September 1947 ahead to, especially, 1948.

[17] Group I, the 2 volume set of MKG translations are found in the Venona collection at 3337/box 17 (not the same as the oft-cited D017); Group II, the XYs, are from D017.

VI. US–UK PROGRESS 1948–1952

One more early collection (annotated as "correct up to 18 Nov 52") gives us totals, though not by year. These are in a binder labelled "New York Summary of Texts" which contains, in order of message date, Meredith Gardner's summaries of NY <—> Moscow KGB messages sent from 28 April 1944 to 23 Jan 1945.[18] A hand count of these summaries shows the following:

Translations (some informal/preliminary)	:	468
Contents of messages unknown	:	68
Messages missing/lost	:	17

Judging by the final statistics—NY KGB messages translated during the life of the Venona program—Gardner had translated the entire body of readable 1944–45 NY KGB messages by the end of 1952. Thereafter he and the others would re-work and improve those translations and add to them the 1942–43 KGB messages and the messages on other lanes (as well as GRU and GRU Naval).[19]

Meredith Gardner, a linguistic genius, had privately studied Russian in the late 1930's. He devised his own method of transliteration to put Russian names/terms into our alphabet. In other words he did not employ the standard Western transliteration form of the time—he told me he didn't know that such existed; further, he found that his own transliteration scheme was better. He told me that the reader's ear, so important in such matters, was better served by having covername SEMEN transliterated instead as SEMYON, which is the way that Russian name sounds.

Phillip Howse began the so-called XY series of reports to GCHQ on 21 April 1950. Each XY, sent in the name of the SLO Washington, consisted of a covering letter discussing the information that was being found in the KGB traffic and attaching new or revised translations of messages, usually in the form of verbatim, message- by-message translations (though then, as later, many of these were partial translations as all groups might not have been recovered yet or were unrecoverable, that is not matched). Thus XY–11, the basic memo, enclosed individual translations XY–11.1, 11.2 and etc. For the study of Gardner's translations I made a count of a bundle of carbons of these XYs, which were mostly the XY attachments, that had been sent to GCHQ in 1952 as a complete set, in case GCHQ had missed some of the serialized attachments (or they had not been sent in the first place). NSA holds a set of XY–1 thru XY–49 (21 April 1950 to 10 January 1952) including the attachments, as well as later series that accomplished the same purpose.

GCHQ put these XYs onto their pre-printed Comint product forms (the "red ball" forms), sometimes significantly re-translated, sometimes with no change in text but with slightly different footnoting, and other times with virtually no change from the XY. These "red ball" Venona reports would then be released to the GCHQ customer (that is the Security Service and the Secret Service) and to Arlington Hall for distribution there. The FBI representatives in London (assigned to the U.S. embassy) were in the Venona picture but were not used as a dissemination channel. The translation and dissemination picture by mid–1950 was looking something like this:

---

[18] Venona Collection in 3337/box 17. This summaries in this binder are very helpful for a quick look-up of a message, especially to learn the state of the translation as of late 1952 (and what hadn't been translated as of that time). Each summary enry contains the cryptanalytic worksheet number and the S/NBF/T number (see the discussion of that term)—using the latter one could probably put the translations in date order and gain some idea of year by year production, but not for years prior to 1950 or 51.

[19] The 1944–45 material was in system [redacted] "easiest" to exploit because it involved a one-part codebook and a very helpful KGB key indicator system. The [redacted] system (the 1942–43 messages) had a two-part codebook and a more difficult indicator. The final statistics for translation of NY KGB messages = 418 messages of 1944 and 51 of 1945.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

1. Gardner, as the only linguist-translator at ASA on the problem (Howse, though involved in every phase of analysis, was not a Russian linguist) would prepare a translation and pass it to Bob Lamphere of the FBI—verbally or as typed by him on ASA/AFSA product form. Perhaps Lamphere would also get the related XY—for example, a translation numbered XY–11.2 (as described above).

2. The translation would be sent to GCHQ as an XY.

3. The XY would be revised/re-translated as appropriate and published as GCHQ product (on the red ball form) in the so-called NBF series: NBF stood for Nichols/Bodsworth/Fitzpatrick and meant the item was Venona. Those three were at that time the principal Venona analysts/translators back at GCHQ and the use of this personalized identifier for a particular product series was very much in the GCHQ tradition—we recall the ISCOT series, GRU or COMINTERN illicit worked by Professor Scott; and the World War II ULTRA series known as ISOS, meaning Illicit System Oliver Strachey, named for the chief of the unit working German intelligence service communications. The NBF would be shipped back to ASA/AFSA and disseminated in the U.S. In other words, Bob Lamphere got a preliminary translation directly from Meredith Gardner and then later a more formal NBF—again from Gardner who disseminated that GCHQ product.

A discussion of translation statistics and procedures is important to understanding the pace and timing of the Venona exploitation, and to understand the translation records— where we find a high percentage of formal translations issued by GCHQ, for traffic on US <—> Moscow lanes concerning American spies (even the final formal translations of most of Gardner's early effort, i.e., everything he did seems to have been re-done by GCHQ). There were several reasons for this latter circumstance, including differences in Russian language training and experience, different requirements of the customers in the U.S. and UK, and format traditions and experience. Some comments on this follow.

While Philip Howse was a cryptanalyst rather than a Russian language crypto-linguist, his successors as the Venona integrees in the U.S. were intensively trained and highly skilled Russian linguists. As only one of them at a time was in the U.S., the other(s) were back at GCHQ ready to give a second opinion on the translations prepared at Arlington Hall. Patrick FitzPatrick served as integree from about April 1951 into 1953, succeeded by Geoffrey Sudbury who held that position April 1953–May 1956.[20] Sudbury and FitzPatrick (and Sir Peter Marychurch) graduated from the first Joint Services Russian Course, Cambridge University, that ran from approximately September 1945 to July 1946.[21] The course director was Professor Dame Elizabeth Hill (M.A., PhD, D. Litt. and now Professor Emeritus of Slavonic studies at Cambridge). Over 100 service personnel attended this inaugural course.[22]

Therefore, Meredith Gardner, privately tutored but mostly self-taught in Russian, with a preference for his own system of transliteration and a varying, sometimes discursive style of footnoting the translations, was in a sense "outnumbered". As far as I have read, and heard from the many interviewees at both centers, none of this caused animosities. The needs of each country's customers were met with this mixed system of reporting.

[20] In his Venona Study, Mr. Vincent says that FitzPatrick replaced Howse on 25 April 1951. Sudbury was followed by Howard Vincent 1956–1959 [redacted] 1959–1962. AFSA and NSA people going in the other direction to serve as Venona integrees at GCHQ were Joan Malone Callahan *1950–55, Meredith Gardner 1955–1958* and H.W. "Bill" Kulp, 1958–61. While expert Russian linguist Patrick FitzPatrick was at Arlington Hall the linguists working Venona at GCHQ included Sudbury, Geoffrey Furniss and Howard Vincent.

[21] Mr. Sudbury gave me a detailed account of this course, and an annotated photograph (personal discussions in Maryland 11 May and 15 July 1992 and letter of 31 August 1992).

[22] Geoffrey Sudbury notes that other attendees included (with their later titles) Sir Michael Hanley, Director General of the Security Service; Admiral Sir Peter Ashmore; Sir John Harvey-Jones and many other people who made careers at GCHQ and in the other intelligence services (in the annotation to the class photo, Geoffrey identified some 16 GCHQ people.

(b)(3)-P.L. 86-36

VI. US–UK PROGRESS 1948–1952

Nor should we discount the impact of the early compartmentation at Arlington Hall (especially 1947–1949) and the dissemination catchup. By the time the XY series was begun in 1950, many earlier translations had gone out by a different route, such as from Arlington Hall to the FBI in Washington and then from Bob Lamphere to the local British Security Service/Secret Service representatives (some of this may have been verbal only) in transactions that might have been unknown to the GCHQ integree at Arlington Hall. For example, in XY–20 of 2 January 1951, Howse told GCHQ that the "pressure of other work here" had slowed down the re-working of the New York —> Moscow texts, "issued a long time ago and seen by Peter Dwyer [the Secret Service representative in Washington] but not forwarded to you." In that same letter, Howse wrote that, "now that you *have the* traffic [presumably a set of the matched KGB traffic] you can rework them in your own order of priority."

GCHQ's customers expected to receive formal Sigint reports according to a known and accepted format.[23] Thus, the NBF series became the definitive series of translations for GCHQ's consumers. Geoffrey Sudbury, in a letter to GCHQ 22 Sep 1953, sumarized the differing views on translation: "I do think there is a slight difference between the immediate targets of the two Centres", for GCHQ wanted to publish as many formal translations as possible to give its customers "background"; at NSA the emphasis was on recovering text that might lead to the identification of cover names, "and no effort is diverted from this to the time-absorbing task of producing formal translations." The FBI had expended an enormous amount of effort in trying to identify covernames and wanted to press ahead as fast as possible (apparently Meredith Gardner used a 60% rule: when a translation reached that point of completion he got it to Lamphere, updating it thereafter).[24]

We close this section on translations by describing the procedures that were in effect during 1953–1956.[25]

- Sudbury or Gardner typed the translation on plain paper with carbons.
- One copy kept by the NSA Venona unit.
- One copy given to Lamphere or his FBI successors.
- One copy by air bag to GCHQ.
- About 3–4 weeks later, a formal GCHQ NBF based on the above returned to NSA by air and a copies of this would be retained for file and given to Lamphere.

D. Lamphere's Covername Study and CI Progress

On 23 June 1950, Bob Lamphere sent Meredith Gardner a long study on covernames in KGB communications.[26] This study, especially when read with Oliver Kirby's briefing notes of late 1949, and

[23] These comments on translations and formats are based largely on coversations with Sir Peter Marychurch, Howard Vincent and Geoffrey Sudbury. Meredith Gardner told me that he accepted the British re-translations as according with their procedures, and he recognized that their Russian language people might translate the material differently. He described the British translations as more literary; his were at once literal but also academic—he footnoted various linguistic possibilities, more so than his British colleagues.

[24] Sudbury's comments are in FP/9, 22 September 1953, in the Venona Collection at 3337/box 18. This box contains the FP series 1–100, corespondence from the Venona rep to GCHQ.

[25] As described by Geoffrey Sudbury in discussions of 15 July 1992 with Benson and Phillips.

[26] Lamphere uses the term "code name" rather than covername, a matter discussed earlier in this study. Lamphere's study is in the Venona Collection, 50–025, box D045.

Gardner's Special Report #1 of 1947, gives us an accounting of all the covernames found in the traffic and those identified up to a certain date.[27]

This was one of many reports Lamphere gave to ASA/AFSA in support of the Venona effort—Gardner would give Lamphere translations containing covernames; Lamphere would then control the FBI investigation or analysis aimed at identifying the KGB agents concealed by those covernames and send summaries of FBI findings to Gardner. Lamphere's reports in turn helped Gardner with further bookbreaking and translating. It was a two-way cooperative counterintelligence effort. Lamphere (or Wes Reynolds) gave ASA fourteen reports in 1948; thereafter Lamphere gave Gardner 40 items in 1949, 77 in 1950, 67 in 1951, 52 in 1952 and 61 in 1953.

Lamphere prefaced his 46 page covername study with a description of some of the patterns of KGB covernames, drawing attention to a few that could only be seen as a category after an identification had been made, e.g., a covername that resembled the true name; a covername that seemed to be a translation of a true name into another language. Lamphere also noted that a covername might be re-used and assigned to another individual.

Lamphere listed 64 covernames that had been positively or tentatively identified, including Russian officials and KGB officers; U.S. public officials not under suspicion; other Americans apparently working on behalf of the KGB. In the latter category we find 34 names. He listed 206 unidentified covernames, many believed to be KGB agents. In the final section Lamphere grouped the covernames, with true name if known, by their affiliation or espionage target, for example (using his headings and identifications as of 23 June 1950):

Individuals Mentioned in Connection with Infiltration of U.S. Government

Covername	**True Name**
ROBERT	Nathan Gregory Silvermaster
DORA	Helen Witte Silvermaster
DONALD,PILOT	William Ludwig Ullman
KANT	Mark Zborowski
LU	[name withheld]
SIMA	Judith Coplon
STUKACH	Joseph Katz
ZORA	Flora Don Wovschin

For some reason Bob Lamphere did not include covername ALES in this list, though in another section of the study he had written that "it is believed that ALES may be identical with [Alger] Hiss. If this tentative identification is correct the close relationship between the [covername] ALES and his true name Hiss can readily be seen." ALES is undoubtedly Hiss—the KGB probably used the GRU's carelessly chosen covername because Hiss was a long-time GRU agent and not (yet?) one of theirs. More of which later.

Lamphere's report identified two KGB agents involved in the effort to spring Trotsky's assassin from a Mexican jail (BOB= Robert Owen Menaker and HENRY=Floyd Cleveland Miller) and listed the unidentified covernames who had tracked defector Viktor Kravchenko during 1944. He listed five people identified from

[27] Oliver Kirby's eleven pages of handwritten briefing notes, prepared at the end of 1949, give specific dates for counterintelligence breakthroughs up to that time. These are in D017.

Venona as being involved with atomic bomb espionage, including REST/CHARLZ= Klaus Fuchs. He reported that unidentified covernames LIBERAL and ANTENNA, along with other unidentified covernames also seemed to have been working that target for the KGB. He noted in a separate section that LIBERAL/ANTENNA controlled a group of at least 9 other KGB agents.

Four days after he sent his study to Gardner, Lamphere added a one-page update which included the statement:

> *Since the referenced memorandum was prepared it has been determined that one JULIUS ROSENBERG is probably identical with the individual described as ANTENNA and LIBERAL.*

The original leads which resulted in the identification of Julius Rosenberg and his net had come from Venona (the same for Fuchs). As we discussed earlier, the covernames ANTENNA/LIBERAL had been found by Meredith Gardner in 1947. In Meredith's opinion, G–2 first identified Rosenberg as a likely candidate for ANTENNA/LIBERAL. A section on Julius Rosenberg and other atomic bomb spies found in Venona appears in the case study chapter of my study (but limited to quoting and summarizing the Venona decrypts—not re-telling the Rosenberg story.)

Oliver Kirby's briefing notes give us another contemporary status report, this dating to late 1949. Some of his information is historically important in dating cryptanalytic and counterintelligence events (from the Venona standpoint).

Kirby's notes highlighted Meredith Gardner's earliest breaks, including the atomic energy scientist message and covername ROBERT's access to top secret War Department documents. He included a good translation of the bribery-in-the-White House message of 1944, noting that the translation was made 8 July 1948.[28] He gave these dates for FBI identifications of particularly important Venona covernames:

- Greg Silvermaster (ROBERT) and Ludwig Ullman (PILOT), November 1948, based on 1947–1948 decrypts of messages of 1944 and 1945.
- Judith Coplon (SIMA) 21 February 1949, based on 1948–49 decrypts of a series of KGB messages July 1944–January 1945.
- Klaus Fuchs (REST, later covername CHARLZ) identified 25 August 1949 based on a series of KGB messages 15 June–14 November 1944, that had been broken in, mostly, 1948 and 1949.

[28] The Presidential election was in November 1948.

Joel Barr was still being carried in Kirby's report as a possible identification for ANTENNA/LIBERAL.[29] One item in Oliver Kirby's notes is particularly interesting in hindsight—quoting from his notes:

> *KATZ was in contact with agent EARL BROWDER (covername HELMSMAN) and also had dealings with AMADEO SABATINI (covername NICK) the go between for JONES ORIN YORK (covername PETE)*[30]*, an engineer in the NORTHRUP Aircraft Company . . . . .*

York was a long-time KGB agent. One of York's handlers was, as stated, Amadeo Sabatini. Sabatini's predecessor as KGB handler for York would soon be identified as Bill Weisband, an Arlington Hall subordinate of Kirby's who had been assisting Gardner and others on various aspects of the Venona and other Russian problems.

[29] Which confuses the issue of who identified Rosenberg when. Both Gardner and Kirby told me that G–2 identified Rosenberg as ANTENNA/LIBERAL before the FBI did.

[30] Actually, York's covername in Venona was IGLA (NEEDLE), not PETE.

VI. US–UK PROGRESS 1948–1952

(THIS PAGE INTENTIONALLY LEFT BLANK)

VII. BILL WEISBAND AND KIM PHILBY

A. Introduction

The story of Kim Philby's espionage has been recounted in a great many books. My purpose here is to discuss Philby's connection to Arlington Hall and Venona and to summarize the appearances of Philby and covername HOMER (Donald MacLean) in Venona. Merely doing that is rather complicated, as it once again involves the Gouzenko case and the matter of the missing traffic. I will make no effort to even summarize Philby's career.

The Weisband story, however, is less well known and warrants very close study. The records are imperfect: discarded, missing, incomplete. Therefore this account will leave many questions unaswered. Weisband probably preceded Philby in the service of the Soviet Union, and he was arrested before Philby was even a suspect, in fact while Philby was on Secret Service (MI–6) duty in Washington and in liaison contact with Meredith Gardner at Arlington Hall, and with Bob Lamphere. We have no reason to believe Philby and Weisband ever met and have no information about Philby's possible interest or assignments, on behalf of the KGB that is, in the Weisband case. But both had access to Venona and presumably turned over what they knew. Weisband in fact had access to all of Arlington Hall's Russian program, at least to the end of 1948 or so when compartmentation within the program came into effect (inspired by the belief that espionage might be taking place!). For our purposes then, the Weisband story will be more detailed (and speculative).

B. Wes Reynolds Alerts Carter Clarke about Weisband

Bill Weisband

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

On 12 April 1950, Wes Reynolds, FBI liaison to G–2, visited Carter W. Clarke, Chief of ASA, at Arlington Hall. Reynolds told Clarke that ASA employee William W. Weisband was apparently a Russian spy.[1] Clarke told Reynolds that Weisband was no longer employed by ASA but had joined AFSA (also located at Arlington Hall) when that organization had been formed in 1949. Clarke recalled that Weisband had married another ASA/AFSA employee at about that time. Clarke said that he would notify Admiral Stone, Director of AFSA, about Reynolds' information and arrange further discussions.

Beginning on 15 April 1950, Bureau agents conferred with officials at Arlington Hall and learned the following:

- Weisband, born in Alexandria, Egypt in 1908 entered the United States in 1925 (or 1929) and became a citizen in 1938. He lived in New York and then in Los Angeles. He was inducted into the Army in 1942, later commissioned into the Signal Corps, and began his association with ASA in 1943.

- Frank Rowlett recalled that Weisband had worked for Colonel Harold Hayes in North Africa during World War II, when Hayes had headed Army cryptologic activities in the Mediterranean Theater (Hayes had preceeded Clarke as head of ASA). Rowlett said that sometime after Hayes returned to Arlington Hall (February/March 1944) to head the Sigint operations division, Rowlett had told him he needed a Russian linguist. Hayes then arranged for the transfer of Weisband from the Mediterranean to Arlington Hall. After the war Weisband stayed with ASA as a civilian employee and had remained in the Army Reserves as an officer. Rowlett said that Weisband had access to extremely sensitive information and could have been the source of serious leaks of information.

- Admiral Stone and [redacted] said that Weisband was working the Russian [redacted] target at AFSA: Russian military, naval and civil internal.

- Carter Clarke and Rear Admiral Joseph Wenger (deputy director of AFSA) told Wes Reynolds that they had feared a leak at ASA/AFSA because "the Soviets changed their domestic systems everytime [Arlington Hall] made a break into them."[2]

Although the records are not clear on this point, we may assume that the FBI told Clarke and the others that Weisband had been involved in espionage on behalf of the Russians before his affiliation with ASA in 1943. At that point the Bureau could not have reported anything about Weisband's espionage activities after 1942. Except for some later information from a KGB defector, that is the state of our knowledge today. We have significant information about Weisband's espionage activities into 1942 when he entered the Army (though even that information leaves many gaps). Thereafter, we can speculate and make some informed guesses,

[1] In this chapter I have generally dispensed with source footnotes insofar as the investigation of Weisband is concerned. During the course of research for this study I gathered various relevant papers, from retired records of the NSA Office of Security and elsewhere. I have generally cited interview sources, Venona material and some current inquiries conducted for me by the Office of Security. Carter Clarke headed ASA from 10 January 1949 to 31 May 1950. I do not know the reason for this short assignment. He later commanded an Army depot in Japan (during the Korean war) and then briefly served at CIA where he fell afoul of Alan Dulles.

[2] We have found no record of ASA/AFSA inquiry into a leak. In a memo for the record written in 1965, Frank Rowlett recalled that when high echelon Soviet traffic went off the air during 1948 "an immediate investigation was undertaken to determine if compromise or penetration was the cause" but that the formal findings of ASA/NSG had been that the Russian action was "generated by the action of their own communications security personnel who had realized the inherent weakness their cipher practice." But Rowlett and others (including Carter Clarke, then in G–2) believed in the "probability" of a penetration. However, there is a memorandum from the Navy's N–202 to N–2 on 26 October 1948 entitled "The Pattern of Soviet Conduct in Connection with Service Cryptography and Communications" [redacted] which is a cover letter to a study of events surrounding the Soviet order of 25 August 1948 ". . . directing the maximum possible use of land-lines for the transmission of enciphered dispatches." In general, the study concludes that there is no clear evidence of a "leak" and that the changes are commensurate with reasonable security moves by the Soviets.

(b)(6)

especially in light of the shocking Sigint losses of 1948. There is even a chance that we have found Weisband in Venona.

The FBI interviewed Weisband in Washington on 9 and 13 May 1950 and in Los Angeles on 16 August. He was suspended from AFSA on 12 May 1950. Mrs Weisband, completely innocent in this matter, was likewise suspended and soon resigned. Weisband denied to the FBI that he knew anyone in the Communist Party or who had been engaged in espionage. He denied removing classified material from Arlington Hall or disclosing classified information to unauthorized persons. He declined to give a signed, sworn statement denying that he had been involved in espionage activities. On 12 August 1950 he appeared before a Federal Grand Jury in Los Angeles that was investigating West Coast Communist Party and Russian espionage matters. Ordered to return for further testimony, he apparently did not exactly follow the instructions of the Grand Jury. He was subsequently arrested, and on 1 November 1950 convicted of contempt. He served one year at the Federal Labor Camp, McNeill Island, Washington. He never made any admissions to the FBI and was never tried for espionage.

C. The Weisband Espionage Case: The Torn Photo of Shirley Temple

In the Fall of 1943, an FBI surveillance team saw suspected Russian intelligence officer Gregory Kheifits, the Soviet Vice-Consul in San Francisco in contact with Amadeo Sabatini (see Chapter III for the "Anonymous Letter of 1943" to the Director, FBI that named Kheifits as a senior KGB officer).[3] Sabatini, an Italian-born American citizen was a relative rarity: a KGB agent who actually knew something about the Working Class (he had been a miner, foundry worker and general manual laborer in Pennsylvania). He served with the Abraham Lincoln Brigade during the Spanish Civil War. In 1949, Sabatini was found in the Venona traffic (covername NIK) and the Bureau moved in on him. Among other things, he told the FBI that he had handled an agent in California named Jones Orin York. York had by then been identified as Venona Covername IGLA (NEEDLE). The FBI then went after York, interviewing him on 10 April 1950 (in Los Angeles) and after. York had this story to tell.[4]

(b) (6)

York, born in Illinois in 1893, briefly attended a teachers' college and moved to California in about 1910. In 1935, he joined Northrup Aviation corporation. In that year he met a group of Russians from the Soviet Government Purchasing Commission who were touring a Northrup factory. The Russians took him to dinner, got him drunk and otherwise laid on the camaraderie. One of the Russians, Stanislau Shumovsky, a tech rep from the Central Hydro-Aerodynamics Institute in Moscow (and a KGB officer) asked him for some aircraft data and paid him a small amount of money. In 1936, Shumovsky introduced him to his KGB handler, "Brooks", who seems to have been [redacted] (recruited by Shumovsky in 1934). Thereafter he passed to another handler, known to him as "Werner", who was Zalm??? ranklin of Milwaukee. Franklin and his father, a doctor, had served in Spain with the Lincoln Brigade. Sometime during 1941, "Werner" told him that he would be getting a new contact who would identify himself to York by showing him half of a torn photograph of Shirley Temple. "Werner" thereupon produced a photo of Miss Temple, tore it in half and gave York his part.

[3] In a 20 September 1944 KGB message not broken into until 1956, Moscow Center warns KGB San Francisco (The Resident —Kheifits) that "According to information received by us intensified surveillance is being directed against you personally". (M —> SF, No. 306, 20 September 1944. Venona Collection box D015). We do not know Moscow's source for that information.

(b)(1)
(b)(3)-P.L. 86-36
(b)(7)(E)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

One evening in August or September 1941, this person appeared at York's apartment on North Harper in Hollywood and gave him the other half of the Shirley Temple photo. He said that his name was Bill, and then or later gave a last name that sounded something like "Vilesband".[5] York subsequently identified a photograph of William W. Weisband as "Bill Vilesband". He also pointed out Weisband to FBI agents outside a federal building in Los Angeles (picking him out of a crowd).

Weisband in fact was already known to the FBI and G–2 (thus the photograph to show to York). In 1948, the FBI had learned that Weisband had been in touch with a suspected California Communist Party functionary. The FBI may not have learned for some time where Weisband worked, for G–2 first heard about this in an FBI letter of 22 September 1949. The FBI then opened, or had already opened, a government loyalty program/communist party type case. An espionage case was not opened until York told the FBI about Weisband in April 1950. Existing records do not show if G–2, ASA or AFSA had any particular concern about the 1948–1949 information. However, Oliver Kirby told me the following.

G–2 had independently taken an interest in Weisband (probably in 1949). Coloney Forney, chief of the Security Group in G–2 had started a program at Arlington Hall to encourage personnel security oversight. Two sources at Arlington Hall secretly reported to Colonel Forney that they had some loyalty and suitability concerns about Weisband. Based on that information some action was taken to restrict his access.

[5] York originally said this meeting was in 1940, rather than 1941. Later he told the FBI that he could date the first meeting as having taken place a month or two before he purchased a camera with money from Weisband. The FBI tracked down the dated purchase record.

I believe the FBI may have closed their case, and in any event Weisband was the subject of a non-derogatory Army background investigation in early 1950.[6] Interviewees included Frank Rowlett, chief of the AFSA Operations Division, Maurice Klein, assistant chief and Waldo Dubberstein, then at CIA but formerly of ASA. Klein and Dubberstein were social friends of Weisband.

Weisband and York remained in contact from August/September 1941 until the second half of 1942 (York said the latter part of 1942—Weisband was inducted into the Army in September 1942). At their first meeting Weisband asked York if he could continue to obtain information. York said that he could but that he needed a camera. At their second meeting Weisband gave him "about $250" for that purpose. On 15 October 1941 York purchased a Contax No. 3 camera with an f1.5 Sonnar lens at a camera shop on Wilshire Boulevard. He paid $257. Over the next year he met Weisband at a number of locations including the Florentine Gardens in Hollywood, Sunset Boulevard, at a bar near the corner of Wilshire and La Cienga, and the Garden of Allah.

Weisband gave York a shopping list of the information the Russians wanted—aircraft specifications, information on armaments, radar and other electronics, for example. He said they were not interested in military bases. York photographed documents (such as the specifications for the P–61 Black Widow fighter) or gave Weisband written or verbal summaries. Weisband paid him about $1500 for his services. Weisband, at their last contact, told him that the next handler might be a woman and gave York identification instructions (note: whoever the KGB might have had in mind then, the next contact was Amadeo Sabatini).[7]

C.1 Weisband in New York 1920s–1941

The second eyewitness evidence concerning Weisband's clandestine activities came from a woman who had been his girlfriend in New York before he moved to Los Angeles.[8] This person reported that she met Weisband in late 1937 or early 1938 in a dance hall in New York City and their close relationship continued into early 1941. Weisband told her that he engaged in secret work that she was not to reveal to anyone else. He said that he was well compensated for this work. His secret work involved delivering and receiving packages according to a pre-arranged schedule. Weisband told her that he did not always know the identity of his contacts—sometimes they were persons he had never met before. She did not actually observe these contacts, but sometimes would wait in a car or her apartment while Weisband made a contact. Weisband told her that his principal had not been pleased to learn about his romantic involvement with her and had made some inquiries about her. He told her that "they" would kill him if it became known that he had been confiding in her.

She saw Weisband in Los Angeles in late 1941, and he indicated to her that he was wondering if he would be able to continue his secret work after he got out of the Army (he wasn't inducted until September 1942 anyway).

(b)(3)-P.L. 86-36

[6] I have not been able to find a complete copy of the background investigation, only extracts. However, we have two Statements of Personal History completed by Weisband: August 1949 and 28 March 1950. The Army background investigation took place between those two dates and is therefore unclear why Weisband completed the second Statement of Personal History. Colonel Forney's interest in Weisband may relate.

[7] York told NSA CI officer [redacted] that Weisband said that "Stan" was his boss, presumably Stanislau Shumovsky though he never used the last name. York recalled Shumovsky as tall, intellectual type who spoke with a British accent. The Bureau believed that Weisband was run out of NYC but that does not conflict with Shumovsky as local handler. Shumovsky was involved in the early stages of the running of Boris Morros (see Chapter XIX.) The woman who might contact York—the covername JULIA (Olga Klopkova) of Venona, or maybe Elizabeth Zubilin?

[8] Name withheld.

(b)(1)
(b)(3)
OGA

CIA

VII. BILL WEISBAND AND KIM PHILBY

Weisband lived in New York from the time he entered the U.S. in 1925. He usually worked as a hotel auditor/accountant.[9] He also worked briefly at the New York World's Fair of 1939. On 1 November 1938, Weisband was arrested by the NYPD for harboring an illegal alien, John Frank Pollock. The charge against Weisband seems to have been dropped. Pollock was released on bail. Later investigation, in light of the other disclosures about Weisband, made it apparent that Pollock was a KGB illegal. The FBI was never able to find him in spite of considerable effort during 1950–60.

We note one other interesting circumstance from Weisband's time in New York: he attended the RCA Institute from 1936 to 1939 studying engineering and radio operation.

D. Information from Anatoli Golitzyn

Golitzyn, a middle-grade KGB officer, defected with his family, [redacted] in December 1961. His later handling by James J. Angleton continues to cause great controversy, especially as he eventually was given access to certain U.S. files to jog his memory and help him in his CI research. However, in March 1962, that is within 3–4 months of his defection and before (presumably) he had access to "memory enhancing" papers, he gave this information to the FBI (expanded upon in July 1962, but not in any material way):

In the summer of 1952 while in the UK–US directorate at KGB headquarters he happened upon a controversy between officers of the Political or Scientific Sections of the American department on the one hand and and that department's counterintelligence section on the other. The discussion was over who would handle an important agent who might be reactivated by the KGB. He recalled a telegram NY KGB —> Moscow that indicated the New York Residency had heard from this former agent. From that telegram or otherwise, he learned the following about that agent:

- He had served a short jail term in about 1949–1950.
- Subject had furnished valuable information to the KGB and had worked in a U.S. "ciphering or deciphering" service.
- Subject was in the military during the war.
- Subject had furnished good information up to the time of his arrest.
- Subject had a connection to New York City and the West Coast; he may have been born or lived in Alexandria, Egypt and had a Russian background.

Too perfect perhaps?

[9] A rough outline of Weisband's employment: 1931–36, Waldorf Astoria Hotel; 1936–38, fulltime(?) RCA student; 1938–39, Hotel Murray Hill; 1939, World's Fair; 1940–41, Stork Club and thereafter the Hotel Miramar in Santa Monica and the Hotel Clark in Los Angeles.

E. Weisband in ASA and AFSA 1943–1950

Lt. Bill Weisband, c. 1943.

Weisband was drafted into the Army on 1 September 1942. He attended Signal Corps OCS from 22 January 1943 to 24 April 1943 and was commissioned a Second Lieutenant. A classmate in that OCS class, Arthur J. Levenson (later a senior executive at NSA) was surprised when Weisband said he would be assigned to Arlington Hall. Levenson had some doubts about Weisband's background, especially his foreign birth (and possibly some other factors too—Levenson had been an enlisted man at Arlington Hall so knew what the place was all about).[10]

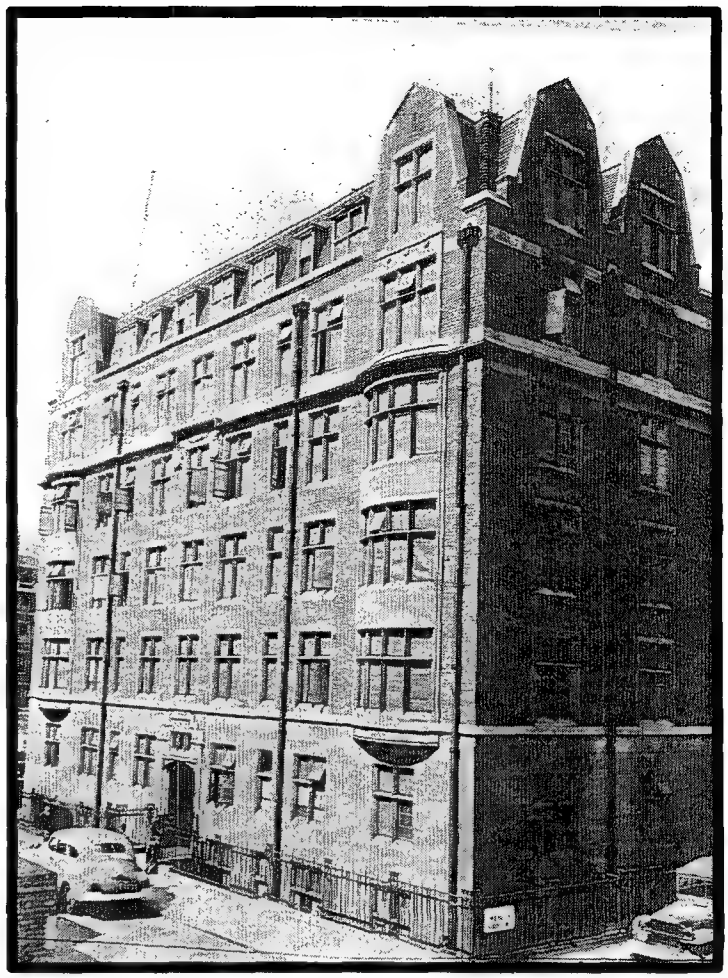
From 10 May to 5 June 1943 Weisband attended an admininistrative and supply course, probably at Fort Monmouth. From 3 June 1943 to 6 July 1943 he attended the Advanced Radio Communications School at Arlington Hall for "9604 training", which at that time seems to have been divided into three separate paths:

- 9604G—Cryptanalytic Officer: German translator
- 9604J—Cryptanalytic Officer: Japanese translator
- 9604I—Cryptanalytic Officer: Italian translator

We will discuss this in another section where we search for Weisband in Venona. Levenson, by the way, ran into Weisband at Arlington Hall and was amazed to see him (Levenson told Bob Farley in 1980 "they should have listened to me").

[10] Cecil Phillips discussed this with Levenson during late 1991 and the latter mentioned his knowledge of Weisband at a NSA History Symposium in October 1991. See also Bob Farley's interview of Levenson, 25 November 1980, NSAOH 40–80, CCH.

VII. BILL WEISBAND AND KIM PHILBY



U.S. Army Sigint Hq Europe, Weymouth St., London. Bill Weisband was there in 1943—was ZVENO?

The date and place of his initial overseas deployment is also important to that section. Enough to say here that he landed in Scotland in July 1943 and after a week there was with HQ SIS/ETOUSA in England, in London, from about 27 July to 3 September 1943. Thereafter he was assigned to the 849th SIS, the Army's Signal Intelligence control group for the Mediterranean Theater, from 8 September 1943 to September 1944. He was back in CONUS on casual status by 14 September 1944. His 849th SIS assignments included about two months in Algiers and Morocco and nine months in Italy (December 1943 to end of Aug 1944). During his assignment to the 849th SIS he met Colonel Harold Hayes who was in charge of Theater Sigint for the Army. Hayes returned to CONUS in February 1944, so their contact would have been sometime between September 1943–February 1944.

(b)(6)

While extensive 849th records have been preserved, mention of Weisband is limited to a roster entry and probable reference to him by position and assignment. In 1950, the FBI interviewed Colonel Hayes and one other officer for some background information about that assignment. Army counterintelligence records concerning Weisband have not been found (which means we do not even know if the Army conducted a CI investigation after the case broke in 1950, or left the matter completely to the FBI).[11]

A roster of the officers of the 849th SIS dated 8 September 1944 lists 2nd Lt. William W. Weisband, but does not describe his duties. At that time Weisband was about to depart or had just departed for CONUS. Another roster of officers, this one with full details about each assignment, and several staff papers about the future deployment of the 849th, were prepared just after Weisband left and so make no mention of him.[12]

[redacted] a wartime Signal Corps officer, recalled for the FBI that he had been Weisband's commanding officer in Italy. He said that Weisband had headed a cryptographic unit in liaison with the Free French and had done an excellent job. A Monthly Report of the 849th SIS dated 3 October 1943, without naming them, says that two officers from the unit and a French officer had been examining recently arrived cryptographic material, "going into every aspect of the security features of the M–209A system. These three officers will, in the very near future, make a series of visits to the French Corps to ensure that the proper handling of the system is known to all concerned." In a report of 3 December 1943 we read that a team consisting of two officers and 12 enlisted men had been sent to the French Expeditionary Corps.[13] In addition, surviving fragments of some notes apparently taken (in the early 1950s?) from Weisband's now lost military records show these assignments:

- Security officer, cryptanalytic and liaison officer, Fifth Army, with French Corps, Crypto team #11, 18 November 1943 to 12 January 1944.
- Security officer, cryptanalytic and liaison officer, French Corps, 12 January 1944 to 18 July 1944.

Weisband, therefore, seems to have been involved in not only cryptographic but also cryptanalytic liaison with the French, the latter duty probably involving some assistance in conducting or obtaining tactical Sigint.

We recall that Frank Rowlett told the FBI that he had asked Harold Hayes for a Russian linguist, and Hayes had arranged for Weisband to be transferred from Italy to Arlington Hall. When interviewed by the FBI at Fort Richardson, Alaska in 1950, Hayes said that he had requested Weisband's services back at Arlington Hall because he was a linguist qualified in French, Russian, German and probably Italian. Maurice Klein would later say that it was his impression that Colonel Hayes had put Weisband into the Russian unit at Arlington Hall in 1944.

Weisband detached from his liaison assignment with the French in July, serving briefly (probably in a casual status awaiting orders or transportation) at AFHQ headquarters. From 7 to 12 September 1944 he was a special courier for AFHQ, which probably meant that he carried classified material back to CONUS. He went on casual status/leave from 14 September to 21 October 1944 and then reported to Arlington Hall.

Frank Rowlett told me that Weisband arrived without having had "the usual CIC security check for SI duty". Rowlett told Colonel Hayes that this was irregular, but he (Rowlett) did not object to Weisband's assignment.

---

[11] NSA Office of Security records have some probable CIC extracts re Weisband, but these are clearance type items, not counterintelligence investigative reports. [redacted] of the CI Division of the NSA Office of Security checked all possible Army/DOD indices, including the Army's central counterespionage case index and found nothing. He found a small Weisband file in the military records center at St. Louis—a very limited service record.

[12] Papers on the 849th SIS are in the NSA Archives at CBLH 12 and elsewhere.

[13] Ibid. These reports are signed by [redacted] was probably his exec.)

(b)(6)

(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

Hayes vouched for Weisband in lieu of security approval. However that may have been, Weisband had been cleared for cryptographic duties in April 1943 and presumably could not have taken the officers' course at the Advanced Radio Communications School at Arlington Hall in June–July 1943 without some kind of approval for access to intelligence information.[14] Rowlett believed that Weisband had probably been a "go-fer" for Colonel Hayes in North Africa–Italy, and Hayes liked him.

One story from that time has it that Lt. Coudert and Bill Smith had both objected to Weisband's assignment to their unit because of his foreign birth and connections.[15] However, Mr. Coudert told me that while he may have interviewed Weisband upon his arrival, he had no objections to the assignment (nor did Smith as far as he knows). Coudert recalled that Weisband knew Russian well and ocasionally made grammatical suggestions to Coudert when they spoke in Russian. Weisband was "no intellectual", but he was a pleasant person who came to small parties given by Lt. and Mrs. Coudert at their apartment in Washington.

It is not clear if Weisband went directly into Smith's Russian unit. Lowell Derbyshire (a Major during the war) told the FBI in 1950 that Weisband had been in his unit during later 1944 and had gone into the Russian unit in early 1945. Derbyshire headed the Romance Languages target effort. Weisband knew several Romance languages so that is not unusual—except that we recall that he had supposedly been brought back to Arlington Hall because of his Russian language capability. However, he had just come from Italy where he had worked with the French, places and languages of interest to Derbyshire.[16]

Weisband's professional duties at Arlington Hall as and officer and civilian remain a bit vague.[17] Gene Grabeel recalled Weisband as a "floorwalker" and that "he just wandered around; he was friendly and good natured, but he did absolutely nothing". Meredith Gardner recalled him as somewhat of a busybody. And so forth. Nonetheless, most recollections are that he was a gregarious person and no one had any suspicions about him. He was not heard expressing radical views. Many recall that Weisband sold jewelry at Arlington Hall. His father (d.1936) and then his brother Mark had been in the jewelry business. After Mark died (about 1946) Weisband began selling rings, bracelets and watches from (presumably) his late brother's stock—he carried these items around in a chamois bag. Most items sold for under $100.

Weisband frequently went to New York, and Cecil Phillips recalls that he bought a new Buick in 1947 and drove to Los Angeles in it. Weisband told Ruby Roland (now Caporaletti) that he was driving the car to the West Coast where he would re-sell it for a profit.[18] Weisband talked about his family's jewelry business from which he had an inheritance. He mentioned having been born in Egypt. His statements of personal history list residences in Alexandria, Egypt; New York, California, and the Washington area, and that his father had been

[14] The Army's security standards for assignment to cryptologic duty had, since 1939, included the requirement that the individual be a U.S. citizen, "preferably native born". Background Investigations for the ASA predecessor organizations had been conducted by the FBI into 1942, and CIC took over then. Persons interviewed for this study report different experiences in this area. Cecil Phillips knew from neighbors' remarks to his family that someone was conducting a background investigation on him (1943). Gene Grabeel, the co-founder of the Russian Sigint program, arrived at Arlington Hall within a few weeks of her initial interview, before security processing was completed (or even started?) Interim security clearances must have been common.

[15] Our source for this information worked very closely with Bill Smith. She repeatedly told us that Smith did not want Weisband in the Russian unit.

[16] In June 1955, Maurice Klein gave Wes Reynolds, Director of Security at NSA, yet another version of Weisband's initial assignment to Arlington Hall. Klein was administrative assistant to Frank Rowlett in later 1944 and in that capacity he had some responsibility for personnel matters. Colonel Hayes called him into his office and told him to find a job for the recently-arrived Weisband, preferably in the French unit. Later Weisband was transferred to the Russian unit. Cecil Phillips and I believe that he was probably in the Russian unit in about January 1945.

[17] Cecil Phillips and I spoke to many people about Weisband attempting to pin down his access and assignments and learn about his background and personality. Cecil himself recalled the most useful information.

[18] Telephone conversation between Ruby Roland Caporaletti and Cecil Phillips, Februrary 1993.

(b)(3)-P.L. 86-36

born in Russia and his mother in Roumania. He mentioned some boyhood travel in Europe with his family. On various forms and records Weisband indicated excellent speaking ability in Russian and French and fair to good in Italian, Arabic, Spanish and German. He could read and write all of these.

KGB agent Jones O. York is our only source of information for other travel possibilities. In 1960 [redacted] an experienced counterintelligence officer with the NSA Office of Security, interviewed York. York told him that at their meetings Weisband took notes in Arabic for security purposes, writing on the margins of newspapers. York also said that Weisband talked about the trouble the Russian government had in controlling diseases in their Asian republics; he mentioned Khazakstan; he said he had travelled in some of the outlying areas of the Soviet Union for "them". Weisband said the Asiatics were not amenable to modern methods. He also mentioned travel in Iran and Turkey. York also recalled that Weisband talked a lot about the need for a Second Front to take pressure off the Red Army. He said that "our people are dying by the thousands because nothing is being done". Weisband's "people" being the Russians. All of which makes Weisband look like an illegal, though I don't think he was.[19]

Bill Weisband standing at center, arm on Gordon Summers' chair. L to R: N. Murphy (USN),; u/I; L. Betts (G–2 liaison); Herb Conley; Hazel Mitchell; Madison Mitchell; B.K. Buffham; John O'Gara, G–2 liaison; Larkin (G–2 liaison); Oliver Kirby; Moe Klein; Tom O'Brien. A party at Arlington Hall Officers Club, c. 1949.

19 [redacted] of the CIA Office of Security assisted [redacted] in this interview which took place at York's residence in the Los Angeles area).

(b)(1)
(b)(3)
OGA

(b)(3)-P.L. 86-36

(b) (3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

Weisband made a lot of friends at Arlington Hall, many of them in positions quite senior to him. However, they were his contemporaries, often fellow officers who shared his overseas experiences. Colonel Harold Hayes seems to have been a social friend throughout this time. Stories have been passed along about them having drinks and conversation at the Arlington Officers' Club (where Hayes lived for a time). A photograph at the club taken in the later 1940s, shows Weisband standing in the front center of the picture, his arm on the shoulder of Gordon Summers (some suggest this photo may have been from Weisband's wedding reception) and flanked by many ASA/AFSA/NSA notables including Herbert Conley, Hazel and Madison Mitchell, B.K. Buffham, John O'Gara and John Larkin from G–2 liaison, Oliver Kirby (head of the Russian problem), Maurice Klein and Tom O'Brien. Maurice "Moe" Klein had succeeded Sam Snyder in running the Japanese Military Attache problem during the war. Later he became assistant to operations director Frank Rowlett and then Director of Personnel at NSA. Klein was Weisband's best friend at Arlington Hall and was best man at his wedding.

A few specific examples of Weisband's activities at Arlington Hall, all of them, in retrospect, quite sinister.

Lowell Derbyshire recalled that Weisband had always been willing to work odd hours and to fill in for others. Cecil Phillips recalls that Weisband spent a great amount of time sitting with the secretary of the Russian unit—who typed virtually all of the section's reports. Another source told Cecil that Weisband said that he would like to review any interesting papers that passed through the unit.

In 1970, Joan Callahan, who headed the Venona effort in the 1960s and 70s, conducted an informal inquiry about Weisband for the Deputy Director (in response to some questions from [redacted][20] She recalled that Weisband had conducted Russian classes in 1945–46 (perhaps as assistant and successor to Ferdinand Coudert). Of particular interest, Mrs. Callahan learned from Ray VanHouten, head of the cryptanalysis subsection in the Russian unit in the late 1940s that VanHouten (in 1947) gave frequent detailed briefings to "high officials" on the status of Russian systems that had been broken and the prospects for breaking others and that:

> *He (VanHouten) used charts, actual overlaps etc in his presentations. He says that after these briefings, while his materials were still out, W. used to wander up and press him for further details, for explanations of how the depths were actually solved etc. Van didn't think that he caught on very quickly.*

Weisband had several other opportunities to "catch on". Meredith Gardner told me that Weisband stood behind him and looked over his shoulder as Gardner filled in the worksheet to book-break the famous NY —> Moscow message no. 1699 of 2 December 1944: the list of atomic bomb scientists. As we have described, Meredith broke that message on 20 December 1946. Therefore, Weisband was on hand to observe the beginning of Venona. (And we should mention that a version of this incident has appeared in some books, but Kim Philby is substituted for Weisband, and the message not specified. The source of this mixup is probably a misunderstanding by Peter Wright.)

[20] That inquiry produced some seriously misleading information that may have been passed on to GCHQ. Such an inquiry, of course, should have been conducted by the NSA Office of Security. We will discuss some of this later, and in an appendix.

VII. BILL WEISBAND AND KIM PHILBY

Ruby Caparoletti, Bill Smith's secretary. Weisband asked her to show him anything interesting that passed across her desk.

(b)(3)-P.L. 86-36

Ruby Roland Caporaletti, employed at Arlington Hall 1943–1956, became Bill Smith's secretary in 1944 and stayed in that position when Oliver Kirby took over. She recalled that Weisband would stand behind her and look over her shoulder as she typed reports. He asked her to show him anything interesting that passed across her desk. She remembered Weisband as a friendly, sociable person. For example, in spite of his junior position, he gave a party for all the ASA section chiefs and their secretaries. She believed that Weisband's closest friend may have been an Army major in G–2 at the Pentagon (not one of G–2's liaison people at Arlington Hall).[21]

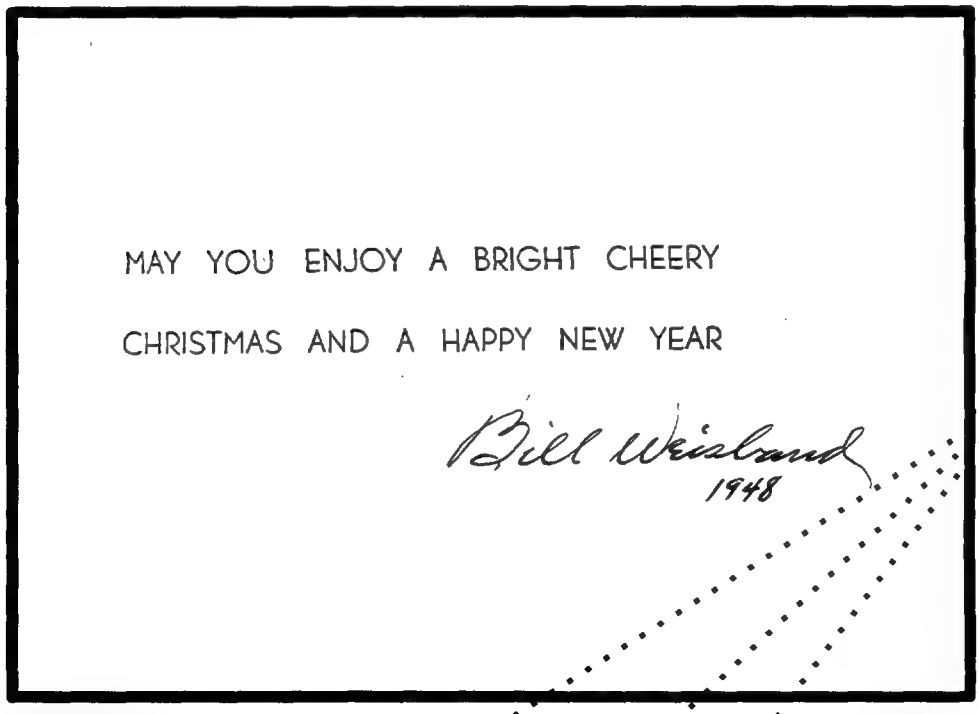
[redacted] recalled another interesting episode. [redacted] who had served in the ASA element at GCHQ, returned to Arlington Hall in early 1948 and joined a staff element under Frank Rowlett that produced statistical and status reports. In one of her first assignments she prepared a special monthly report, Eyes Only for Colonel Hayes, on the status of the agency's cryptanalytic programs. Weisband asked her for a copy of this report, but she told him that she could not do so on her own authority. Weisband assured her that he had always seen this particular report in the past.[22]

---

[21] Interview of Mrs. Caporaletti by Benson and Phillips on 23 February 1993. Mrs. Caporaletti could not recall the name of Weisband's close friend in G–2. Our attempts to identify him weren't successful.

[22] Cecil Phillips' discussions with [redacted] on 4 and 5 November 1992. [redacted] said another person, who was away at the time, usually prepared this report. The other person told [redacted] that Weisband had seen these reports in the past—that person had given or shown the reports to Weisband because he didn't have enough work to keep himself occupied. We have not specifically identified this series of reports beyond what [redacted] told Cecil Phillips.

VII. BILL WEISBAND AND KIM PHILBY



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Bill Weisband's holiday greetings, 1948, to Helen O'Rourke, secretary to Oliver Kirby, head of the Russian problem.

Cecil Phillips, Meredith Gardner and Gene Grabeel all recalled how Weisband had helped them administer the mock Venona cryptanalytic problem used in training new people.[23] Miss Malone (the later Mrs. Callahan) and Miss Grabeel had a number of new people who needed training [redacted] Up until that time, the practice was to give new analysts real material to study. This proved unsatisfactory so Cecil suggested, or someone suggested to him, that they should create a realistic problem for training these new people. Grabeel and Malone picked Red and Green [redacted] (Trade) code texts which they juxtaposed and enciphered with either synthetic key or some previously solved key to produce [redacted] Mr. Gardner then created two pages of pseudo [redacted] (KGB) code which was placed in depth against the [redacted] text. Cecil Phillips coordinated the machine assistance. Bill Weisband pitched in to help the new people solve the problem.

Organization charts, 1946–49 show Weisband's official assignments (charts for later 1944 do not show him and the 1945 charts are too general, though he is on a late 1945 roster listing all officers at Arlington Hall).:

- 14 May 1946. Weisband is on the Language Staff of WDGSS 93–B (the Russian unit). Captain William E. Brown was director, and James K. Lively the deputy director of this staff.
- 5 June 1946. Weisband is listed as assistant director of the Russian Language Staff.
- September 1947. Weisband is shown on both the Language Staff and the Russian Military and Air Unit of the General Cryptanalysis sub-section (headed by Dr Dubberstein and Ray VanHouten).

[23] Cecil Phillips prepared a paper on this matter for me to use in this study. My account of the mock problem is based on that paper (with a few items from my discussions with Gardner and Grabeel).

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

- November 1947. Same.
- February 1948. Weisband shown as a member of the Russian Language Staff.
- June 1948. Weisband is deputy head of the Scanning sub-unit of the Russian Plain-Text sub-section.
- December 1948. Weisband holds the same position. The Scanning sub-unit (headed by Constantin Oustinoff) now included some 55 people.

On 15 November 1948, Commander E.W. Travis, Director of GCHQ had written Harold Hayes about the sudden disappearance of high grade traffic:

F. Russian Systems Possibly Compromised by Weisband

At this point we will not speculate any further on the probable compromise of the Venona technique, but will review the non-diplomatic systems that disappeared soon after exploitation began or was about to begin.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

Cecil Phillips prepared the following description of these systems, with an evaluation of the potential for compromise by Weisband.

[24] NSA Archives at CBKI 58 in a folder labelled OP–20 Staff memos.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[redacted]

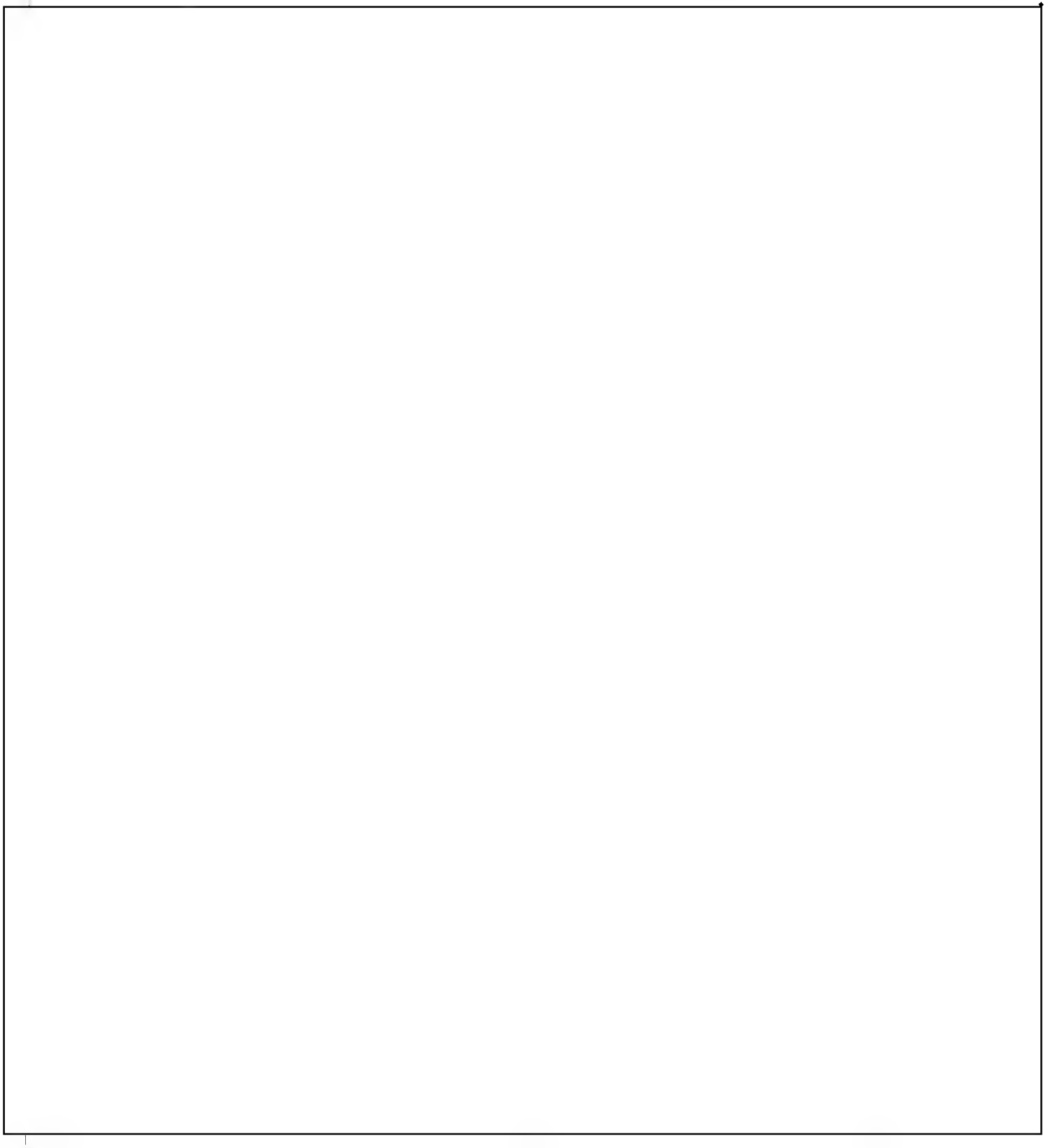
It does not seem that Weisband (or any other source) could have had much direct effect on the cryptography of this problem —but he might have helped "kill-off" the use [redacted] in favor of random lists in October 1949 because the nature of this work was certainly known to him simply because it consumed the efforts of up to 20 or so people at one time in an open section to which he would have had access.

[redacted]

There don't seem to be any records of Weisband's role with respect to [redacted] but Cecil Phillips is almost certain that he did a lot of the translation. For a time he was assigned to the Russian military unit, and in any case he was, supposedly, the best Russian linguist, available to any individual or element needing help.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

[redacted]

SUMMARY

While none of these system changes can be absolutely attributed to Weisband, he had all the access he ever needed to destroy virtually everything that was done on the Soviet problem from 1945 to about 1950. It appears that no one ever suspected him, even though many former members of the section recall as does Cecil Phillips that he was nosy and wandered around a lot. However, there was some explanation. For two or three years he was the section's senior linguist (in skill if not position) and it was his job to help out anyone who had a linguistic problem. Further, he almost certainly did many translations and probably had access to every report which was published in multiple copies for distribution. Since there were no close checks on documents, it would have been as easy as one could want to take documents out at night, photograph them and return them in the morning with no one being the wiser.

There seems little doubt of Weisband's part in the system "deaths" of 1948—[redacted] However, there

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

is absolutely no way to determine whether new pads were issued or whether the code clerk simply moved into a new batch of pads already on-hand.

G. Is Weisband in the Venona Traffic?

The best way to start trying to answer this question is to first put Jones O. York in the middle, looking at his appearances in Venona and the appearances of his handlers other than Weisband. Except as noted, all referenced messages are KGB.

Jones O. York. Covername: IGLA (Needle). York has been found in the traffic four times: San Francisco —> Moscow, No. 446, 31 Oct 1943; San Francisco —> Moscow, No. 457, 2 November 1943; New York —> Moscow, No. 1266, 6 September 1944; and New York —> Moscow, No. 1523, 27 Oct 1944. As we would expect, York looks like an important agent and he is engaged in espionage for money (and he is chronically short of money). He is shown to be connected to covernames KhARON (Grigorij Kheifits, the Resident in San Francisco), NICK (Amadeo Sabatini), DUGLAS (one of several covernames for Joseph Katz). A very quick summary of these messages (some of which will be discussed again in a later section on KGB San Francisco):

- In October 1943, York handed over 5 rolls of film about the "XP–58" and its new motors, and he was in "desperate need of funds for buying a house". In November 1943, San Francisco reminded Moscow of the need to give York $800 for the house.
- A year later (and none of the IGLA messages in between have been recovered) New York KGB told Moscow that Sabatini had stopped meeting York because of possible surveillance. According to the message York was again in need of money (though the message could mean that it was Sabatini who needed the money).
- In the last message that has been recovered, New York KGB discussed sending Sabatini back to California to find York and establish conditions for contact and give him "a perpetual password", after which Sabatini would return to New York and, presumably, someone else would be contacting York. New York KGB also suggested that covername ChEP (who has never been identified) might be a better choice for getting the password to Jones York. Covername ChEP cannot be Weisband as an 18 July 1944 messages places that unidentified person in New York, at a time when Weisband was still overseas.

(b)(6)

Stanislau Shumovsky. Covername: BLERIOT. Jones O. York told the FBI that he had been recruited by Shumovsky who passed him on to other handlers (the first of these was "Brooks", believed to have been [redacted] He has been found in the traffic four times, including once under his true name (in a Moscow —> Washington Trade message of 10 December 1942). It is apparent that Shumovsky specialized in aircraft matters and had, at least since 1938, been getting good information in the U.S. As of 8 July 1942 he operated under the cover of the Aviation Department of the Soviet Government Purchasing Commission. Later collateral reports state that Shumovsky was a career KGB officer working technical matters.

Zalmond Franklin. Covername: ChEN. He handled Jones York before Weisband. He appears in Venona three times but not connected to Weisband or York. Franklin was known to York as "Werner".

Amadeo Sabatini. Covername: NIK; and Joseph Katz. Covernames: STUKACH, DUGLAS and IKS. Katz, especially, is very prominent in Venona and we will discuss him again. As we have seen Sabatini was York's last known handler. Katz was involved with York and Sabatini and almost certainly with Weisband as well.

Circumstances of time and place do not favor finding Weisband in the Venona material. He left New York in the summer of 1941 and made contact with Jones York in August or September of that year. Based on the

information from his ex-girlfriend and the matter of the illegal alien Frank Pollock, we assume he was active for KGB New York prior to 1938. Only one (1) KGB message out of hundreds for the year 1941 has ever been read, and only a few groups of that message could be recovered. Traffic from 1939 and 1940 cannot be matched and has not been exploitable through other means. No Los Angeles KGB (or GRU) traffic has ever been exploitable, and Weisband entered the Army in 1942, serving overseas for more than a year. He was at Arlington Hall in October 1944. The unreadable Los Angeles traffic does contain some interesting possibilities, but we cannot know. [redacted] could be a notification to the Center that Weisband had found York. Pure speculation of course. The traffic boxes in the Verona collection [redacted] But we should add that Weisband may have been under control of New York or the KGB Resident in San Francisco; KGB SF <—> M messages of that time are scarce and unreadable.

We find one covername that might fit Weisband, that being ZVENO (Link, as in link of a chain).

Weisband is a German name. The second syllable of his name "band", can have a meaning like link. The German–Russian dictionary does not define the Russian word ZVENO as the German word "band". But a case might be made.

Covername ZVENO has been found in three KGB messages, the earliest of which strikingly suggests that ZVENO is Weisband. The message, as recovered and translated in 1979 is quoted in full below:[29]

From: New York
To : Moscow **26 June 1943**
No. 981

The last 4 weeks "ZVENO" has spent [1 group unrecovered] school [4 groups unrecovered] ...INGTON, VIRGINIA where he underwent a course of instruction in Italian. By his calculations he will leave the COUNTRY in the first half of July and will arrive on the ISLAND at the end of July. We are setting up the following arrangements with ZVENO:

1) The password for [1 group unrecovered] contact in any place in Russian or in English: our man: "Hullo, Bill. Greetings from Grigorij." He: " [7 groups unrecovered] on the West Coast."

2) Starting from 24 July Z. will wait for our man in LONDON on Sundays on the [1 group unrecovered] at the entrance to Leicester Galleries, Leicester Square and on [c% Wednesdays] [3 groups unrecovered] on the [1 group unrecovered] on the [1 group unrecovered] east corner of Orchard

[41 groups unrecoverable]

Rush the telephone number and your instructions before [1 group unrecovered]

No. 546 **LUKA**

As this message contains all the evidence for the case that Weisband is ZVENO, we'll analyze it sentence by sentence before mentioning the other two ZVENO messages.

- The last 4 weeks "ZVENO" has spent [1 group unrecovered] school [4 groups unrecovered] ...INGTON, VIRGINIA where he underwent a course of instruction in Italian.

[redacted]

VII. BILL WEISBAND AND KIM PHILBY

A footnote to the published translation of this message says that there is some evidence that INGTON is Arlington, Virginia. If we assume that the reference is actually to Arlington Hall, Virginia then it becomes a matter of identifying the course and determining Weisband's whereabouts and language training or ability. We know the following from Weisband's surviving military records:[30]

– As a member of the Officer Signal Corps Replacement Pool, he was assigned to the Advanced Radio Communications School, Arlington Hall from 3 June 1943 to 6 July 1943, for 9604 training.

– At some point in his service career, perhaps during the original interview at Arlington Hall or while in OCS, he rated his language ability as

	speak	write	translate
Italian	well	some	some
Arabic	some	some	some
French	well	well	well
German	little	little	little
Russian	well	some	some

As we noted earlier in this chapter, 9604 training consisted of three separate tracks 9604G (Cryptanalytic Officer German translator), 9604J (Cryptanalytic Officer Japanese translator) and 9604I (Cryptanalytic Officer Italian translator). Both the German and Japanese courses required prior knowledge of the languages; the German course ran for 7 weeks; the Japanese course 18 weeks. Arlington Hall records do not show the length of the Italian course, but it presumably was less. As Weisband's 9604 training is not further specified in the records, we have to assume it was 9604I, Italian, based on the fact that he was in training for about 4 weeks.[31]

• At the moment he has been given leave until the 27th of June [12 groups unrecovered] the ISLAND. By his calculations he will leave the COUNTRY in the first half of July and will arrive on the ISLAND at the end of July.

COUNTRY means the U.S. and ISLAND the UK. The records show that Weisband left CONUS on 17 July 1943 and arrived in the ETO, 29 July 1943.[32] That latter date may be when he landed in Scotland or when he reported into Hq. SIS/ETOUSA in London. This too fits the ZVENO message.

• We are setting up the following arrangements with ZVENO:

1) The password for [1 group unrecovered] contact in any place in Russian or in English: our man: "Hullo, Bill. Greetings from Grigorij." He: "[7 groups unrecovered] on the West Coast."

Once again everything fits. Weisband spoke Russian fluently. His true name and his "street name", as known to Jones O. York was Bill. Grigorij is the true first name (or at least the name he used publicly) of Grigorij Kheifits, the KGB Resident in San Francisco and the senior KGB man on the West Coast, where Weisband had handled Jones York (i.e. Hollywood/Los Angeles did not have a Resident). Finally, ZVENO in his password reply is to mention the West Coast.

[30] Most Army officer records for the period 1912–1947 were destroyed in the fire at the records center in St. Louis.
[31] In later years, Weisband tended to rate his language abilities somewhat higher than he did in 1943 (and I've sometimes used his higher ratings).
[32] These are the dates shown on the form "Record and Report of Separation—Certificate of Service", one of the documents that has survived. Presumably these dates were taken from his records rather than provided by Weisband (as some of the dates I've cited are).

• 2) Starting from 24 July Z. will wait for our man in LONDON on Sundays on the [1 group unrecovered] at the entrance to the Leicester Galleries, Leicester Square and on [c% Wednesdays] [3 groups unrecovered] on the [1 group unrecovered] east corner of Orchard

This part doesn't help us make an identification except that we have to assume that ZVENO must have told the New York KGB that he would be in London and would be able to make some meets.

The other two ZVENO messages don't tell us much. In NY —> Moscow, No. 1239, 30 August 1944, it states: "Your number 3640. Through VOLUNTEER's wife we learned from [probably] ZVENO's brother that ZVENO [12 groups unrecoverable]." VOLUNTEER has never been identified, though in a later KGB message covername SERB (sometimes identified as Morton Sobell) reported that VOLUNTEER had been killed at the front in Europe. [redacted] was living in New York at this time, and we have information that he had Communist connections. If ZVENO is Weisband, then this message might (the unrecoverable part) have [redacted] passing along information about Bill Weisband's anticipated return to CONUS (he returned o/a 9 September 1944).[33]

The final message, Moscow —> New York, No. 154, 16 February 1945 is mostly unrecovered or unrecoverable and the part referring to ZVENO is unclear; "[55 groups unrecoverable] [b% according to a communication from] the naval neighbors ZVENO will await a meeting on 24 February at 9 o'clock in the evening. The place and password [6 groups unrecovered]."

Note that Moscow Center is telling New York KGB information that they have apparently received from the GRU–Naval—ZVENO will be expecting to meet the KGB in New York etc. We really cannot resolve any part of this message in the Weisband context. Weisband had been back in the U.S. for over 5 months. Why would Russian naval intelligence—in Moscow—be informing the KGB of meet planning? The Russian Navy did have observers and the like in the Mediterranean, and in some Italian ports. Perhaps Weisband could have made contact in Naples? Too speculative.[34]

So, is ZVENO Bill Weisband? In keeping with the Venona procedure of, in descending order, footnoting covernames as (true name given), probably (true name), possibly (true name) or unidentified covername, then I would rate ZVENO as "possibly William W. Weisband".[35] A lot fits, almost perfectly, but there are too many unknowns and none of the information in the KGB messages is uniquely Weisband. The matter of the Italian language training at Arlington is perhaps the key—we need to know if OSS or some other agency had Italian language training in Arlington, Virginia or if OSS or others were able to take an Italian language course at Arlington Hall. If not, the case for ZVENO=Weisband gets stronger.

(b)(6)

[redacted]

[35] The discovery that Weisband and ZVENO looked a lot alike came about during the course of this research. CIA had speculated that ZVENO was an OSS type; FBI and CIA suggested a person with a Serbo–Croatian background and gave some names. Later, FBI seemed to rule out these people. NSA/GCHQ always have carried ZVENO as an unidentified covername. During this study we put a major effort into all aspects of the Weisband case and often could not find what we were looking for. Venona veterans such as Mildred Hayes said they had looked for Weisband in the traffic but had found no good suspects. None of the interviewees mentioned ZVENO, and I suspect that by 1979, when the best ZVENO translation was formally issued, the facts of the Weisband case were unknown to the analysts still on the problem.

VII. BILL WEISBAND AND KIM PHILBY

Cafeteria at Arlington Hall. Here, on 4 Feb 1943, Sam Chew ran across Maurice Halperin, the KGB's agent covername ZAYaTs.

A final oddity relating to language training at Arlington Hall and Venona personalities. Covername ZAYaTs (translated Hare or Stowaway) was Maurice Halperin, an important KGB agent in the OSS. He has been found in Venona in at least 28 messages. When we interviewed Dr. Samuel P. Chew, a veteran of Venona cryptanalysis (see Chapter III etc) he told us this remarkable story from his first days at Arlington Hall.

Dr. Chew entered on duty at Arlington Hall on 4 February 1943, and on that day he met Maurice Halperin in the cafeteria. He was shocked to see Halperin at Arlington Hall, as Halperin, a teaching colleague at the University of Oklahoma, was known to him as a member of the Communist Party. Halperin told Chew that he was at Arlington Hall teaching Spanish. Chew recalls that Halperin invited him to social events during that time, but he declined because of Halperin's associations. Chew recalled that Halperin left Arlington Hall for an assignment in Latin America. Dr. Chew could not recall any other circumstances or details of Halperin's work at Arlington Hall.

Maurice Halperin taught at the University of Oklahoma from 1939–41, when he joined the OSS predecessor organization. By the end of the war he was heading a Latin American division of the OSS and also worked briefly for the State Department. I could not find any record of Halperin in a search of ASA records held at NSA (including various accounts of training at Arlington Hall and work on Spanish-language targets). While there would seem to have been no need to train Spanish linguists for Sigint translation purposes (i.e. plenty of Spanish speaking people were available), it seems at least possible that Halperin could have done some teaching

of Spanish fundamentals to new employees who would be screening traffic. We know that elementary French was taught for that purpose; we have seen that a short course in Italian (another non-rare language) was taught.

Venona gives no clues to Halperin at Arlington Hall—the earliest mentions of his covername are in NY>M KGB messages of 11 May 1943 (no. 651) and 22 May 1943 (no. 751). Neither of these has been issued as a translation, presumably because nothing other than a covername(s) could be read. The first translation that mentions Halperin is KGB message NY>M 8 June 1943, no. 880, which gives the Center a list of KGB agents in the OSS.[36]

H. The Weisband Case in Later Years

On 29 March 1951, a Loyalty–Security Hearing Board (relating to Federal employment), meeting in San Francisco concerning Weisband unanimously found that: 1. reasonable grounds existed to show that Weisband was disloyal, and 2. his removal from Federal employment was in the interest of national security.

In September 1951, an FBI analysis of the Weisband case noted that York's last three handlers—Franklin, Weisband and Sabatini—had all been directed to Los Angeles from New York City, which meant that their principal was in New York. Franklin and Sabatini had been controlled at one time by Dr. Gregory L. Rabinowitch; other cases showed that Rabinowitch's agents had later been turned over to Joseph (Jack) Katz. Therefore, Weisband may have followed that same course: Rabinowitch to Katz (and upon reaching the West Coast he may have passed to control of the San Francisco Resident, Grigorij Kheifits). (b)(7)(E)

In July 1953, the Bureau re-interviewed Weisband. He identified a photograph of Jones O. York but refused to discuss him or answer any questions about espionage. Then, as in later years, he complained about the way he was being treated by the FBI. The FBI continued to interview York, clarifying dates and places.

[redacted]

(b)(1) (b)(3) OGA

On 20 July 1960, Wes Reynolds, Director of Security at NSA and James A. Grooms, head of his Special Operations Division visited CIA to be briefed, "by Bill Harvey's organization on Soviet intelligence activities as disclosed by information secured from a special source". [redacted] gave the CIA's briefing on behalf of Harvey; also present from CIA were Colonel Sheffield Edwards, Director of Security; and [redacted][38] We cannot tell from the documentation if [redacted] briefed the NSA visitors on Venona or was talking about information from a defector or active source. The briefing turned to Weisband. [redacted] Wes Reynolds cautioned the group about the need to bring the FBI into the discussions. The really curious thing about this meeting is that the NSA representatives had not known the full extent of the Weisband case—that is, the Office of Security knew about the information from the later 1930s, that Weisband had apparently been a courier for Russian intelligence. They did not know the far more detailed information that Jones O. York had given the FBI some 10 years before.

CIA

---

[36] Cecil Phillips will examine the worksheets (JKB 07 and JKE 40) of these untranslated messages to see if it appears that some text can be recovered.

[37] Earlier Office of Security records on Weisband are incomplete. Some important material was destroyed (or retired to the NSA Archives and not yet re-located). The 1960–66 documentary record is likewise incomplete.

[38] The names are of interest: Wes Reynolds, when with the FBI, got the Bureau into the Venona secret (see Chapter IV.); [redacted] as part of James J. Angleton's CI Staff, was CIA's Venona representative to NSA for many years—he became involved soon after Bob Lamphere quit the FBI and in a sense continued the enthusiastic consumer cooperation and interest in the Lamphere style. Sheff Edwards is well known to students of mole hunting and conspiracy theories.

(b)(1)
(b)(3)
OGA

CIA

VII. BILL WEISBAND AND KIM PHILBY

The transition from ASA to AFSA to NSA, and the resulting changes in security arrangements, seem to have allowed a most extraordinary gap in the understanding of this case.

[redacted]

(b)(3)-P.L. 86-36

(b)(7)(E)

(b)(1)
(b)(3)
OGA

CIA

[redacted] On 11 March 1966, he learned from the FBI Liaison Officer that the Bureau had "no objection to NSA approaching Weisband in an attempt to gain his cooperation and get from him any information he may wish to reveal about Soviet Intelligence." [redacted] later briefed the Deputy Director of NSA about the Weisband case [redacted] That ended it.

Weisband died on 14 May 1967 at Fairfax Hospital in Virginia. He had lived for many years in suburban Virginia, not far from Arlington Hall, working as an insurance salesman and sometime apartment manager. His later years seem to have been quite difficult. He reportedly told a friend that he had been a "scapegoat" and he blamed "officials", not further described, who persuaded him to "become involved"—whatever all that may have meant, if anything.

It would appear that the U.S. counterintelligence interests would have been well served by an approach to Weisband in later years. If Weisband had cooperated, we might have learned more from him than from any other American spy up to then or since, for it appears that Weisband operated on behalf of the KGB from at least the mid–1930s until 1950, and probably again, if only in a restricted way, thereafter: possible illegal, agent-officer, agent handler in New York, Los Angeles and Washington and probable source for [redacted] loss of access to high echelon Soviet systems for many years. We may also assume that he made recommendations to the KGB about other suitable candidates for espionage.

This remains a strange case and one cannot but feel that it was papered over rather too quickly by AFSA. The FBI did not get leads that should have been run: the Bureau never interviewed Meredith Gardner, Cecil Phillips, Gene Grabeel, Ferdinand Coudert, Mrs. Caparoletti and others who could have shed some light on his access, comings and goings and connections. AFSA didn't seem too anxious to get the Bureau too far into what

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Weisband had been working. Within the Bureau and at AFSA, no one seems to have told Bob Lamphere about the true meaning of the case, i.e. that Weisband had been much involved in early Venona.[39]

Finally we have the recollections of Oliver Kirby, head of the Russian problem at the time of Weisband's arrest.[40] Mr. Kirby told me that indeed AFSA had been happy to get beyond the Weisband case as soon as possible and to limit public exposure of the case. Kirby made an assessment of the case. He and his superiors concluded that Weisband had done very great damage to the national security. But he was finally out of access and AFSA could move on. If the full case had come to trial as an espionage case the following could have resulted:

[redacted]

AFSA, said Mr. Kirby, was just as happy that Weisband didn't talk and silently went to jail on the contempt charge.

I. Kim Philby and Arlington Hall: Background

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Kim Philby (STANLEY)

Kim Philby arrived in the United States in October 1949 to take up his assignment as the Secret Service (MI–6) liaison to the FBI and, especially, the CIA. He would replace Peter Dwyer, though they overlapped for some months.

[39] Bob Lamphere told me that he has absolutely no personal knowledge of the Weisband case, in spite of the fact he had been in liaison with Meredith Gardner et al of the Russian unit for over a year before Weisband's arrest. Obviously these were hectic times—espionage cases breaking everwhere, many or most because of Venona. Bob says the FBI would not have compartmented the case, that is, put it in some system not available to him. But it is clear that the Weisband case agents did not know about Venona or much about AFSA's Russian effort. AFSA certainly didn't do much to help. Admiral Stone mentioned to the FBI at the time of the Grand Jury proceedings that he was concerned that Weisband would talk to the Grand Jury about Soviet Intelligence activities!

[40] Kirby discussions with Benson.

[redacted]

VII. BILL WEISBAND AND KIM PHILBY

At that time Dwyer was receiving Venona from Bob Lamphere of the FBI, and occasionally directly from Arlington Hall. Philip Howse, the GCHQ Venona integree at Arlington Hall, kept his headquarters apprised of cryptanalytic developments and translations through his PH series of reports. He sent copies of important PHs to Dwyer at least three times: PH 35, 20 April 1949 went to Dwyer with the approval of Carter W. Clarke, head of ASA; PH 56, 15 July 1949; PH 80, 29 November 1949.[42] As we have seen, Howse started a new intelligence series on 21 April 1950, the XY series under which GCHQ received translations and commentary.

Philby, therefore had access to Arlington Hall Venona from: 1. (presumably) Dwyer's file of earlier PHs and Venona he received via the FBI; 2. Some of the later PH letters, still addressed to Dwyer by Howse, though Philby was on board; 3. All XYs from XY–1 of 21 April 1950 thru, at least, XY–29 of 1 June 1951.[43]

J. HOMER and Philby

Donald Maclean (HOMER)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Meredith Gardner had recovered references to " 'G' Material" in 1947. As the exploitation developed it would be seen that "G", HOMER, GOM(M)ER were one and the same: KGB agent Donald Maclean (at the very beginning it was not clear that "G" was a person—it seemed to Gardner that it could have been a class of information).

[redacted]

[42] Undoubtedly more PHs went direct to Dwyer. But in any case, he was well served by Bob Lamphere and got what he needed. My point in this section is to show how Arlington Hall had a direct connection to the British consumers. This was all very cooperative, that is, Lamphere was kept apprised of all of this by Gardner.

[43] I have earlier given archival location references to the PH and XY series and will not footnote these again. Philby returned to the UK o/a 10 June 1951.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

a wide range of material. Therefore, the initial emphasis on finding a crib for ASA, rather than identifying a (British) spy seems reasonable.

[redacted]

Meredith Gardner produced a short paper on these messages on 1 February 1949.[44] It had been established by then that these Washington KGB messages were quoting British Foreign Office telegrams.[45] Gardner had translated the opening phrase of these KGB messages as "Material G", but he pointed out that the Cyrillic letter in question could be considered three ways:

1. As merely representing the 4th letter of the Cyrillic alphabet—but he noted there was no parallel in which a single letter was used to represent a category of material (in other words there was no Material A or Material B.)

2. The letter initial could stand for Lord Halifax, and thus be an abbreviation for the true name of a major political figure—since Cyrillic contains no 'H' and 'G' is often used for 'H'".

3. The letter could stand for the first letter of the true name or cover name of the person who was passing the British telegrams to the KGB.

The latter possibility soon won out and the appropriate counterintelligence inquiries began. To follow this part of the story to its conclusion, from the standpoint of Arlington Hall, we draw from Meredith Gardner's summary of 11 October 1951.[46] Separate from the Washington KGB traffic, several messages NY —> Moscow were found to relate to this matter. A New York KGB message of 5 September 1944 (No. 1263), which had been partially broken in 1947/48, contained the opening phrase, "According to advice from HOMER [GOMER]", Roosevelt and Churchill would be meeting in Quebec on 9 September. But, wrote Gardner, "there was nothing in the message to suggest a connection with the Washington material of the following year." That KGB message said that HOMER's "resume" of information concerning the Quebec conference would follow. It did, in a KGB message of 7 September 1944 (No. 1271–1274), but the opening phrase in that second message, which contained the name HOMER, was not solved until early Spring 1951.

Another NY —> Moscow message, 28 June 1944 (No. 915) showed that a senior KGB officer had met with someone called GOMMER (as it was said in the message; the message did not say HOMER/GOMER or "G"). Or, as Gardner put it, "It was impossible until actual identification had been made to be sure that GOMMER was the same as GOMER." Quoting Gardner at some length:

> *In August 1950, Mrs [Carolyn Wiley] Gray of AFSA recovered two stretches which read, "work including the personal telegraphic correspondence of [Churchill] with [Roosevelt]" and "weeks ago G. was entrusted with deciphering a confidential telegram of [Churchill's] to*

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

[Roosevelt]". These recoveries were transmitted to the British 11 August 1950, who thereupon set up work-sheets for further recovery work. The suspicion that "G." was the source of material "G" occurred to people at AFSA immediately upon seeing Mrs. Gray's work, and the suspicion was suggested to the British at the same time.[47]

The imaginary hand-off from Weisband to Philby was quite well-timed. Weisband, present at the creation of Venona in December 1946[48] was then able to observe the practical measures by which KGB traffic of 1944–45 was being broken out and read. He worked directly on, and in any case close to, all the major Soviet systems that ASA/NSG and GCHQ broke into from 1946–1948. Every one of these systems went dark, and

[47] Caroline Wiley Gray, a long-time ASA/AFSA/NSA employee worked with Katurah MacDonald as a depth "reader". In other words, she was involved in the immensely difficult work described by Cecil Phillips in Chapter V.

[48] Actually, it was worse than that. Weisband had toured and then joined the Russian unit in early 1945. Without question he would have been briefed on the progress of the Russian Dip program and the fundamental cipher break that Arlington Hall had made at the end of 1944.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

[redacted]

After 1948, Weisband might not have been able to move about quite so freely, but at any rate he was by then in the middle of new sources of Sigint [redacted] At that point Philby arrives, in October 1949, and if he was too late to save Klaus Fuchs (identified from Venona at about that time and arrested in Jan/Feb 1950) he certainly saw a remarkable amount of Venona material, such as:

[redacted]

The covername "KIM" is tentatively recovered in message #100 of 19 September 1945 (22 groups).

The name Kim was found in one message of a small series of Moscow —> London KGB messages that had just been matched. We do not know if this "Kim" was a covername—seen just once and never identified—or an accidental use of H.A.R. Philby's true nickname. It seems possible to assume the latter given the rather hectic and emergency nature of the Moscow —> London messages of that September (though Geoffrey Sudbury does not believe that this KIM = Kim Philby). The earliest published translation of that message that I have been able to find is from March 1956 and in it Moscow Center tells London KGB to, "Please expedite a reply to No. 6244 re the conclusion about 'KIM' ". Moscow's No. 6244 was not intercepted—and it is only fair to point out that the message number would seem to place it before the crisis period.

The crisis of September 1945 had been the defection of GRU cipher officer Igor Gouzenko to the RCMP in Ottawa. Incredibly, almost the only KGB traffic London <—> Moscow that had been preserved, and that was matchable, was from the very time of the defection. The history of that traffic, originally, as we noted earlier in this study, called L <—> M [redacted] is unclear. While it was quickly found to be regular KGB [redacted] rather than illicit or uncategorized Russian Diplomatic, records in the Venona Collection do not tell us how it arrived at Arlington Hall. [redacted] In other words it seems that GCHQ had found a small amount of uncertain, possibly Diplomatic traffic, L <—> M and had offered it to Arlington Hall knowing that the latter was searching around for any and all Russian Dip: In [redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

[redacted]

Once again, the matter of the missing traffic. The reader is referred to earlier chapters for a discussion of whether or not Russian Diplomatic traffic had been taken after June 1941, and if so, if it had been destroyed in the belief that it was unbreakable one time pad material. Whatever may have happened, by 1949–50 it became apparent that the only traffic that could be located had been taken by the British Radio Security Service (RSS) during September 1945. It seems to have been passed in manual morse on national links, that is transmitters in the Soviet Embassy London <—> Moscow. The RSS had, by chance it seems, covered an exceptionally important period. Unfortunately, the quality of the intercept was poor, especially outbound from London. Some 25 Moscow —> London messages, 12–20 September 1945 were broken, most of them, though only in part, quite early. Only a few London —> Moscow messages would ever be read and those in the later stages of the Venona project.[51]

Thus Philby was faced with a series of problems and opportunities including:

1. He was getting a steady feed of KGB covernames and identifications.

2. His nickname "Kim" may have appeared in one of the messages; he knew (or rather his controllers knew) that the matched September traffic included damning references to him.

3. He probably knew that the covernames for Burgess and Maclean and others were in the Moscow <—> London traffic—he could have tracked some of the progress in exploiting the September 1945 traffic.

4. From the Washington <—> Moscow and New York <—> Moscow decrypts and his liaison with his headquarters, the Security Service, and FBI he knew that Maclean was about to be identified.

Philby, unlike his predecessor Dwyer, rarely visited Arlington Hall. Meredith Gardner recalls meeting with him a couple times—he gave Philby some information or progress reports, but Philby in turn had nothing to say. Their meetings took place in a private conference room adjacent to Carter W. Clarke's office. While Meredith dispels the legend that Philby "looked over his shoulder" while he was bookbreaking, he did say in a report written in 1955 that Philby had been present at some of "the conferences we had in the General's [Carter Clarke] suite over the worksheets."[52]

Burgess and Maclean, tipped off by Philby, ran in late May 1951. Shortly after their disappearance Philby, and Geoffrey Patterson of the Security Service, met with Bob Lamphere at FBI headquarters (described by Lamphere in his book). Philby was soon recalled to London. The Venona collection shows a few milestones along this road:

• XY–31 of 2 July 1951 is the last one of the series showing Philby on distribution (he had probably departed by then).

---

[50] The Coast Guard intercept and exploitation unit had been an element of the USN Sigint organization during 1940–45. Commander L.T. Jones ran it for most of that time; Mrs. William F. (Elizebeth) Friedman was a member of the unit. Its specialty was covering Western Hemisphere <—> Germany clandestine circuits of the German intelligence services, and then doing the decryption and translation. This unit made at least one independent break into an Enigma system. [redacted]

[52] Gardner letter to Callahan and Deafenbaugh, 31 October 1955 in Venona Collection at 3337, box 17 (FMC folder). Gardner wrote this while he was the Venona integree at GCHQ. Oliver Kirby also had several meetings with Philby during this time and visited his residence in Washington at least once.

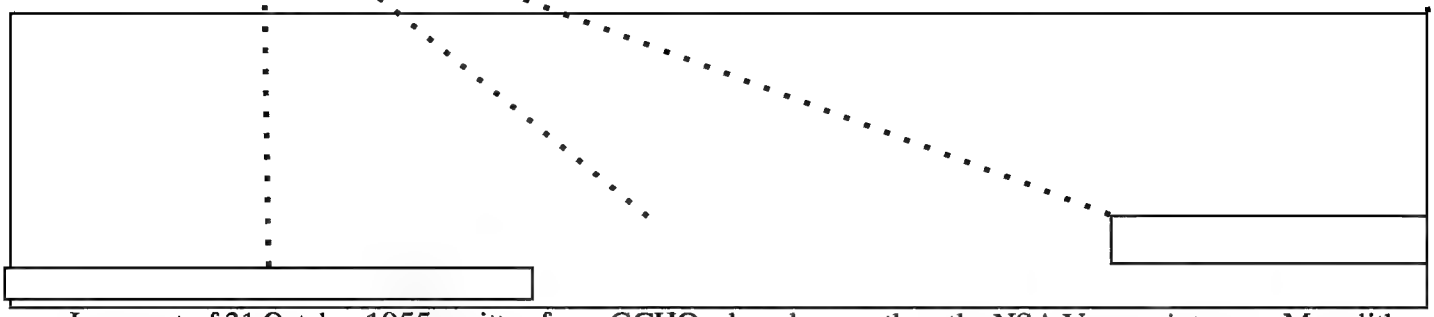
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY



In report of 31 October 1955, written from GCHQ where he was then the NSA Venona integree, Meredith Gardner wrote that MI–5 now thought they knew which of the London KGB covernames was Guy Burgess; Meredith wondered about the identity of covername STANLEY (STENLI), and "how did he come to have access to information about the Gouzenko case?" Gardner continued, "Speaking of Burgess, a curious question was asked in the House of Commons on the 25th of October by Lieutenant Colonel Lipton":

> *LIEUT.–COL. LIPTON asked if the Prime Minister had made up his mind to cover at all costs the dubious third man activities of Mr. Harold Philby, who was First Secretary at the Washington Embassy until a little time ago, and to stifle all discussion on the grave matters evaded in the wretched White Paper which was an insult to the intelligence of the country.*

Gardner then continued, "I can't say just what this means, but I may remind you that H.A.R. ("Kim") Philby .....".

K. Philby in Venona

This section could be an appendix, (or be in the case studies part of this study). However, this case is of such interest that a few more documents and dates seem appropriate.

[redacted]

September 1945. Though Arlington Hall had made the break into both the U.S. —> Moscow HOMER (Maclean) traffic and the Moscow —> London traffic, the latter must have been mostly worked at GCHQ after Spring 1950. However, other sources give us some idea of the recovery of KGB London covernames. STANLEY/STENLI, the KGB covername for Philby seems to have first been recovered in later September 1951 (3 months after Philby's recall). Philby could have known that covername JOHNSON (DZHONSON) had been found by Arlington Hall or GCHQ before he left (that covername hasn't been identified on the translations held in the NSA Venona Collection). The important thing for Philby to learn would have been that the Moscow —> London material of September 1945 had been matched and would therefore, in time, be broken.

The sequence of events in September 1945, had gone like this:[53]

- 5 September. Gouzenko defected in Ottawa.
- 7 September. Gouzenko gives statement to RCMP.
- 8 September (a Saturday). William Stevenson, head of MI–6 in Western Hemisphere notified "C" about the defection. (This is the key date).
- 11 September. London KGB sends long urgent messages to the Center.
- 14 September. Same as above.

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

• 17 September. The Center sends an urgent message to London KGB confirming STANLEY's information about Gouzenko.

London KGB's outgoing messages cannot be read. It must be assumed that their messages of 11 and/or 14 September passed along to Moscow what Philby had learned from "C" about the defection. The Center's reply is quoted as follows:

From: Moscow
To: London
No. 46 **17 Sep 1945**

To BOB

The chiefs gave their consent to the checking of accuracy of your telegram concerning STANLEY's data about the events in Canada in the NEIGHBORS' sphere of activity. STANLEY's information does correspond to the facts.

VIKTOR

In this urgent message Lt. General Fitin (Covername: VIKTOR, head of the foreign intelligence directorate at the Center, that is the First Chief Directorate) advises the London Resident that Philby's information about the Gouzenko defection has been checked with the GRU (the NEIGHBORS) and is true.

No Ottawa KGB or GRU traffic of that time is readable and nor is New York or Washington traffic (some 1945 traffic is readable but none is for the right period, and none mentions this case).

Guy Burgess (HICKS)

The other readable Moscow —> London messages of September include a number of operational security decisions in the wake of the defection and they include covernames that have never been identified. A later study by Geoffrey Sudbury took the number of London's September covernames, and by comparison to U.S. traffic volume and decrypts developed a statistical basis for the total number of probable, but unrecovered (that is never found) London covernames—over 100. Some other interesting decrypts:

• No. 34, 21 September. Covernames JOHNSON, HICKS (Guy Burgess) and STANLEY (Philby) are in the message.

• No. 64, 21 September. The London Resident, BOB, is ordered to exercise special care in meeting with "S."—that is, STANLEY.

• No. 54, 18 September. Refers to a meeting "last week" with STANLEY (that is, Moscow comments on London's meeting)

No. 47, 18 September. Concerns safeguarding the "valuable" agent network in light of the GRU's problems in Canada. Refers to STANLEY, HICKS, and JOHNSON. (GCHQ re-issued this translation 8 times after the original of 30 October 1952).

At least one message refers to atomic bomb espionage, presumably by an unidentified British KGB agent (probably a woman).

We'll mention decrypts of GRU London messages of 1940–41 and 1945–later 40s in an appendix.

Returning one more time to Philby's access to Arlington Hall product, which he saw in the XYs, we note the following.

[redacted]

And, we have discussed the HOMER material available to Philby.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VII. BILL WEISBAND AND KIM PHILBY

(THIS PAGE INTENTIONALLY LEFT BLANK)

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPMENTS DURING THE 1950s

A. Discussion

This chapter concludes Volume One of this study and the (roughly) chronological presentation of the history of Venona. Volume Two will consist of a series of topical or case studies based on the KGB traffic and the translations — with occasional reference to the chronology of exploitation; and Volume Three will cover the GRU and GRU–Naval case studies along with a final chapter on the later chronology of the Venona program.

A purpose of this chapter is to describe the breaks into four systems: the earlier KGB, known to US–UK as [redacted] Ambassadorial [redacted] GRU [redacted] and GRU–Naval [redacted] Until the early 1950s all the exploitation (except on the Canberra <—> Moscow lanes) had been against system [redacted]

We will also discuss other highlights of the Venona program, including the FBI's progress in identifying covernames, and various operational, personnel and policy matters — [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950s

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950S

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950s

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950S

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950s

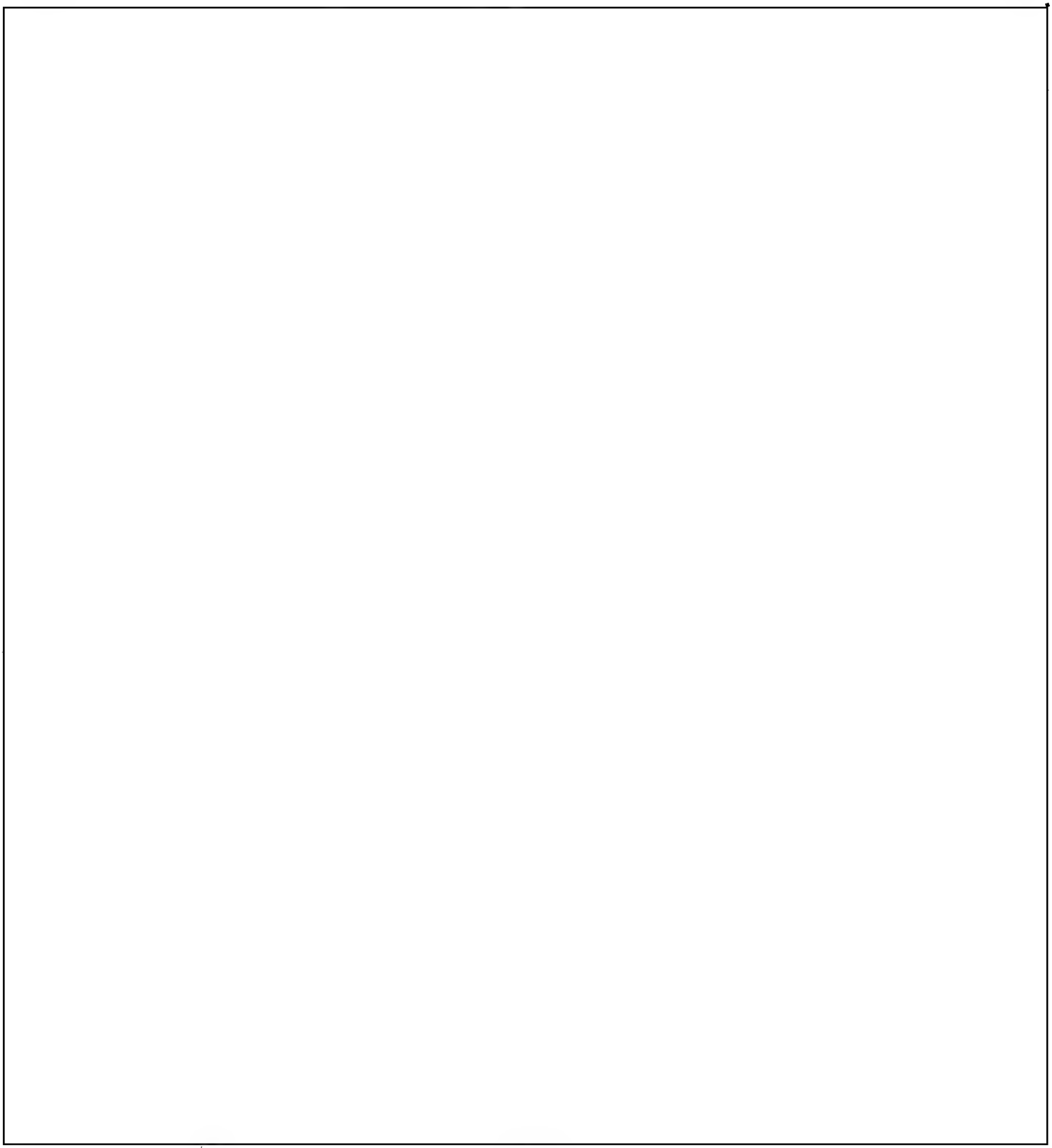
VIII. VENONA DEVELOPEMENTS DURING THE 1950S

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

Dr. Richard Liebler. He developed a new approach to Venona cryptanalysis.

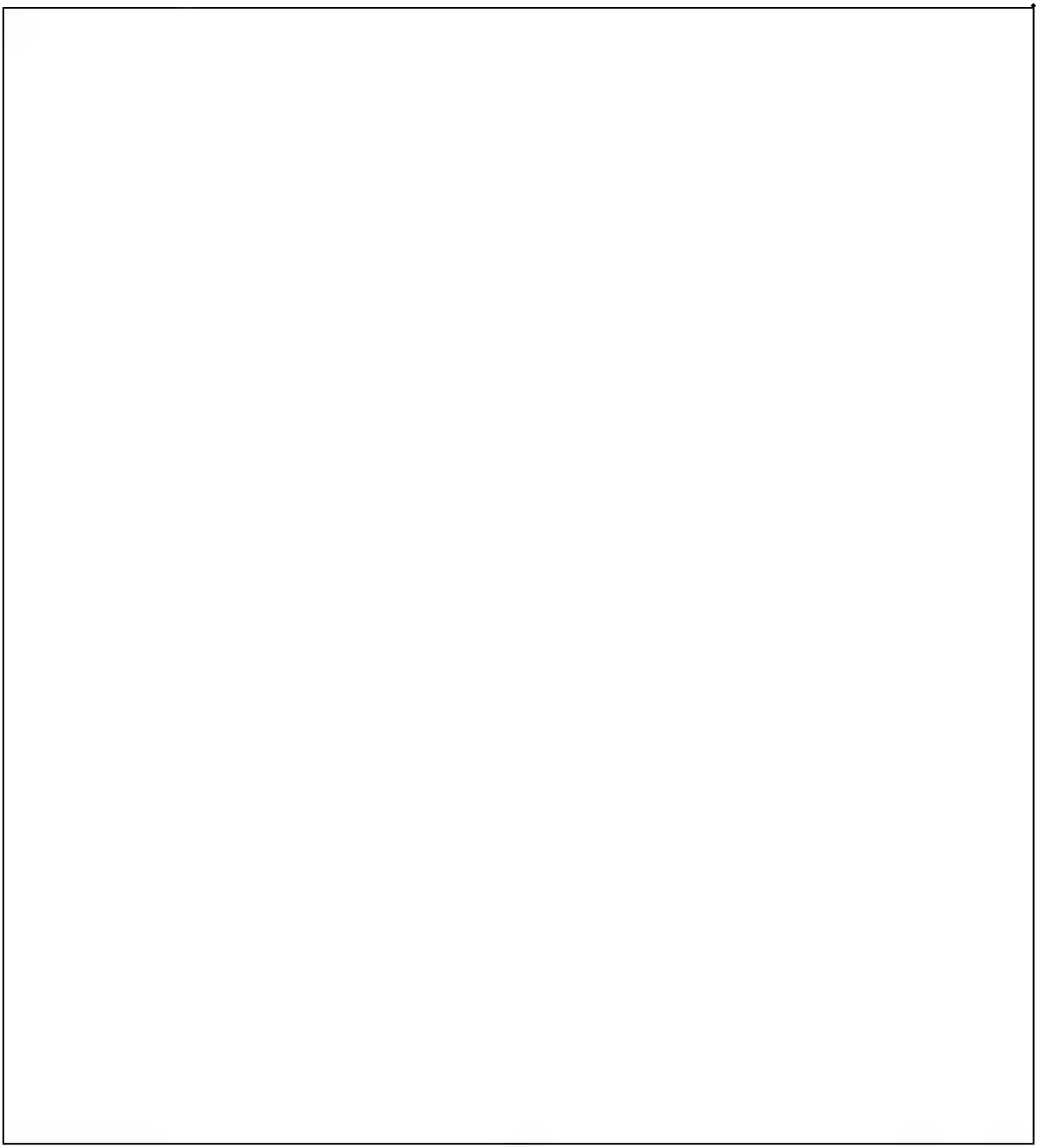
(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950s



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950S

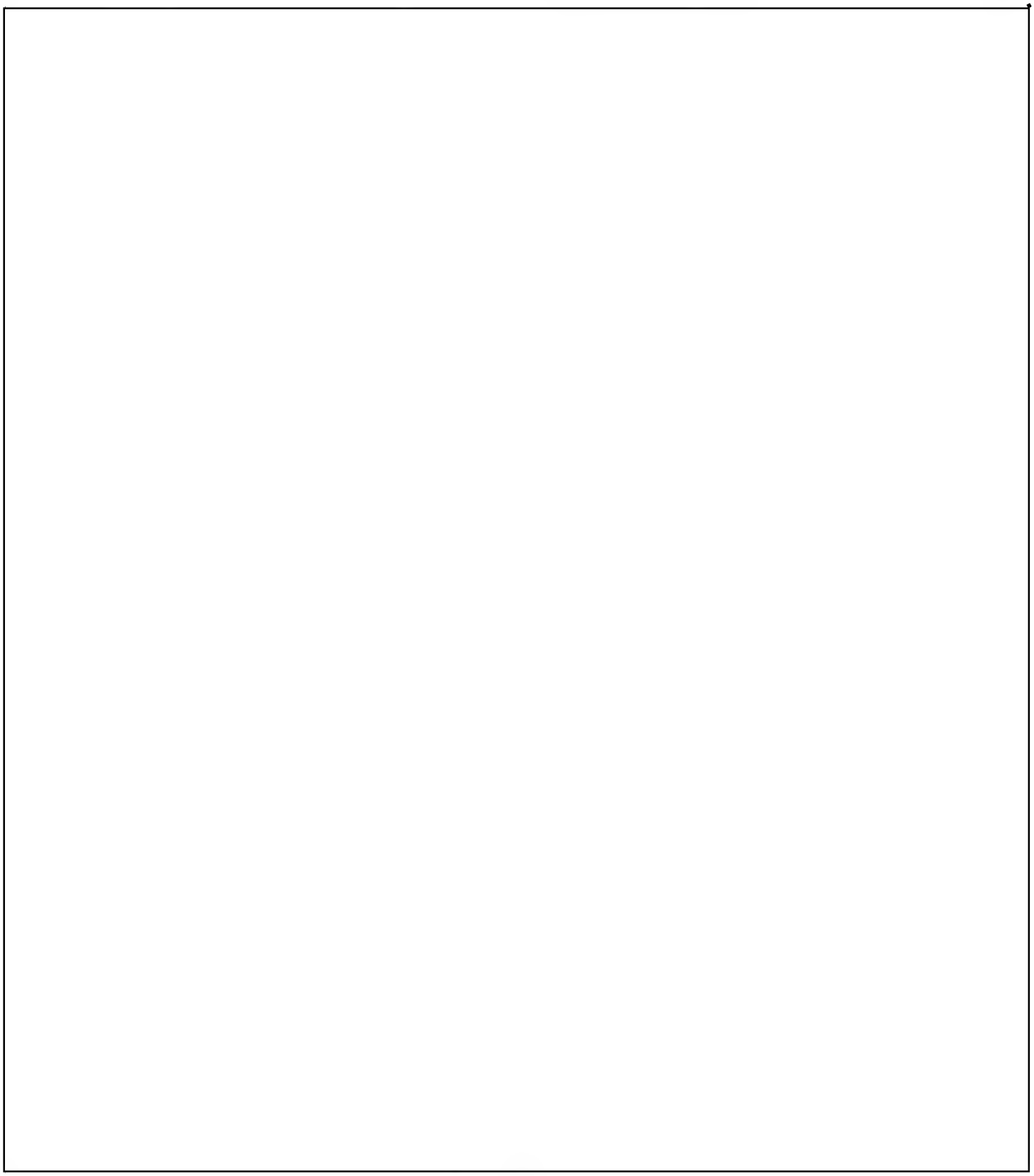


(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950s

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950S



(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950s

F. The CIA

Some CIA personnel had access to Venona as early as 1948, but only to Meredith Gardner's earliest published product, that is, the eleven Special Reports of 1947–48. Other CIA efforts to see some of the material, e.g., messages that might concern the penetration of the OSS, had been rebuffed. ASA and AFSA had not been anxious to continue or expand CIA access.

Meredith Gardner recorded how this changed:

(b)(1) (b)(3) OGA CIA

> *It was obvious that a considerable part of the [redacted] material would interest CIA, and, as has been seen, members of CIA had access to certain reports from... October 1948. No satisfactory way to channel later specific information to the proper place in CIA existed, however, until 1952, when with the help of [redacted] direct liaison between Gardner and [redacted] of CIA was arranged for and the security of [redacted] material at CIA was taken care of.*[16]

We do not have the exact date when [redacted] was read on, but on 18 August 1952, CIA officers William K. Harvey (who has been mentioned in the previous chapter in connection to the Weisband case) and [redacted] were indoctrinated. [redacted] became the CIA Venona representative on 5 May 1955 and remained with the problem for some 20 years (see the Weisband chapter). [redacted] was a historian and Russian linguist, and a member of James J. Angleton's Counterintelligence Staff [redacted] CIA collateral support and CI analysis in support of Venona began in early 1953.

(b)(1) (b)(3) OGA CIA

CIA, therefore, officially entered the Venona problem four years after the FBI.

G. Covernames and Identifications

Volume two will contain a more definitive accounting of message traffic, success rate, covernames and identifications. The following comments help to show the scope of the decryptions and agent identifications into the mid–1950s.

While AFSA had prepared, at GCHQ request, the first systematic listing of all covernames found in Venona, GCHQ seems to have updated the lists from late 1951 on. In their November 1951 covername report on the New York –> Moscow lane, we find a 57 page list containing about 419 covernames and for each the external message number, message date, and US–UK translation number. It would soon become the custom to pencil in, below the covername, the true-name (or the possible/probable true-name).

The New York to Moscow lane was mined quickly and early — in the November 1955 update for that lane, the covername count was about 482, that is, only about 60 new covernames had been extracted from the traffic in the four years since the basic GCHQ listing. This number would increase as the exploitation of [redacted] proceeded (and of course there were the other lanes to study and then the GRU material).

[16] From Gardner's handwritten, unsigned paper on early Venona compartmentation prepared in the 1950s. Venona Collection D017. We have commented earlier on the difficulty Gardner faced during the earlier years of the Venona program concerning dissemination. He received mixed signals.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950S

In 1950, Bob Lamphere had written a study of covernames in Venona from which we can get some idea of the status of agent identifications at that time. In 1952, he followed this with two more reports — these on known or suspected Russian (essentially KGB) agents operating in the United States 1944–45 (in other words, the years of KGB system [redacted] which would remain the richest source for Venona).[17] In one of these reports, in listing all known or suspected spies, Lamphere includes the Venona covernames. From this and study of the traffic we get a reasonable accounting of Americans working on behalf of the KGB, who had been identified through (or found in and thus confirmed) Venona up to mid 1952: about 65 Americans. Of these I believe 6 had been found in Venona up to that point only under their true names. Some 36 probable KGB officers had also been identified from the NY <—> Moscow traffic. These numbers do not take into account Washington, San Francisco or the GRU or GRU naval (however, NY <—> Moscow provides, today still, the majority of the Venona names).

By 1952, many of the more important KGB general operational terms or coverterms used in the Venona traffic had been identified, including "Probationer" as the term for an agent; "Worker" as the term for a KGB officer (at least an officer assigned to a legal establishment).

In 1952, the FBI also produced two reports on Soviet intelligence service communications. Though copies of both were quickly disseminated to the (new) NSA, one senses some dissatisfaction about protocol and channels. That is, the publication "Soviet Intelligence Communications" appeared in non-SI channels. Strictly speaking it did not contain Venona. The sources of information included Gouzenko and other defectors, and information from the FBI's own Sigint, including cryptanalytic, operations during World War II, which insofar as the Russian target was concerned, included the interception of clandestine stations in the Soviet establishments in New York and San Francisco and the exploitation of secret writing.

The second publication, also titled "Soviet Intelligence Communications", dated 4 December 1952 was issued, at the Comint Codeword level — but it had been prepared by the FBI for the British Secret Service (not for NSA). In any event, these are valuable studies and I use them in the next volume.[18]

We should also mention some of the basic documentary work done by the FBI, and later the CIA. Many KGB messages quoted U.S. documents from a variety of agencies, some of which had been reorganized during the war and then disestablished after the war. The FBI, CIA, the British services (and during the later 1940s, ASA people too) made a considerable and usually successful effort to find these documents — which were studied for their CI value but especially for use as cribs in the cryptanalytic process.

H. Some Operational and Organizational Highlights

The two centers continued to discuss the division of work. On 4 February 1953, A.G.Royffe, heading the effort at GCHQ noted to Fitzpatrick that a formal division would create difficulties. He said that as the NSA flow of translations "has picked up again, one of our problems (that our customer was receiving little or nothing for long stretches at a time) is resolved." He said that MI–5 and MI–6 regarded the New York traffic as very important to the understanding of KGB tradecraft. Royffe offered to be flexible as to the production of formal

[17] These documents are filed in D045 and D046 of the Venona Collection: at the former location the report "Summary of Persons Involved in Soviet Espionage for [KGB] in 1944–1945", dated 7 May 1952. The other report is untitled, serialized as 52–052 and probably dates to December 1952. That report, curiously, is typed on AFSA pre-stamped paper. But it is credited to the FBI, so perhaps Lamphere used the AFSA form as a convenience, and considered this document a draft.

[18] See 3337/box 16 and item 52–051, box D046, both in the Venona Collection. The clandestine stations were heard only for part of 1943. The intercept was done for the FBI by the Radio Intelligence Division of the FCC. The FBI had its own cryptanalysis section, which had excellent success against German hand systems and secret writing (but not Enigma or One time pads).

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

translations — during a period when GCHQ might not be able to get these out, Fitzpatrick was to issue them from NSA.[19]

Fitzpatrick reported to GCHQ that the conclusion had been reached at NSA that Moscow message signatory VICTOR was Lt. General Pavel Mikhajlovich Fitin. Generals Deane and Donovan, as we described, had met with Fitin in Moscow in 1943 and described him as head of the KGB's intelligence collection effort. In one of the postwar recoveries of German records, the Army had found a long transcript of German interviews of KGB Lt. Zhigunov, captured in 1941. Zhigunov had described Fitin and said that by 1941 he was heading the external intelligence service.[20] It followed that he would be the signatory and addressee for messages concerning intelligence operations (as we will see, there were other signatories, even including Beria, for other types of KGB messages). In other analytic housekeeping of the time, Geoffrey Sudbury and Meredith Gardner re-translated the FBI Anonymous Letter of 1943.

By late 1953, the NSA [redacted] unit had begun to lose people with no immediate replacements. Between July–November Venona veterans Kay Keen, Caroline Gray, Eleanor Bledsoe, Caroline Fairley and Freda Calvin left the Agency. In a reorganization of May 1954, the Venona activity, then simply called the "Gardner Operation" was placed under Thomas J. Thaler as head of unit 7244–4. However, the special role of Gardner and his associates, in many ways outside a normal chain of command, continued. For example:

> *Mr. Meredith K. Gardner acts as senior consultant and advisor in all phases of the operation. He will continue to act as the primary contact with consumers in matters pertaining to the distribution of COMINT end products of the operation ... Mr. Thaler and/or his superiors will have access to [dissemination] records ...they will not normally be concerned with end product...If an item of such outstanding importance is produced that, in Mr. Gardner's judgement the normal distribution channel should not be used he is authorized to contact directly the Director NSA.*[21]

Katurah McDonald actually headed the operation, with Gardner theoretically subordinate to her as a consultant. The other consultants were Dr. Sam Chew, Raymond Van Houten, and Paul Gerhard, with Geoffrey Sudbury as the GCHQ integree.[22] In all, the immediate Gardner/McDonald operation at NSA then involved 12 people.[23] But, supposedly for security reasons, there was no clerical help. Gardner and Sudbury did their own typing.

GCHQ integration into the entire Venona operation had reached such a comfortable level that Sudbury acted in liasion to Bob Lamphere at times. As Sudbury reported to GCHQ:

---

[19] HX 1/31, 4 February 1953 in 3337, box 18, Venona collection. All references to GCHQ and UKLO correspondence in this section are to papers located in this box.

[20] The translated Zhigunov transcripts seem not to have been available to Arlington Hall for some years after the war. This is a fascinating document — the Lt. had even dictated to the Germans the syllabus for the KGB CI officer basic course (as it was in 1939). The course outline is virtually indistinguishable from courses for U.S. CI personnel — even the administration of the course has a familiar look: a faculty cadre, expert guest lecturers, senior officer speakers; classroom lectures, field problems run by both cadre and students.

[21] Disposition Form dated 13 May 1954, signed by Dr. Lawrence Shinn, Deputy Chief, Office of Analysis. Venona Collection, box D049, in the folder "Persons Briefed".

[22] Gene Grabeel and her group were at that time in a separate depth reading sub-section — concerned with reading [redacted] and testing for matches, outside the inner office where the Venona was produced.

[23] At about this time the GCHQ unit included Bodsworth, Carson, Fitzpatrick, Mason and Vincent, with NSA employee Joan M. Callahan as the integree.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

In Gardner's absence I have been working with Dr. Chew and have given Lamphere translations so that the search for cribs can begin..... P.S. Lamphere has telephoned to say he has found a crib for one of the five messages. This took him [just] 24 hours.[24]

In fact highlights of Lamphere's work with NSA during this period are most easily traced through Sudbury's reports to GCHQ.[25] For example:

As you know, the main target of the FBI is still MER/ALBERT, who is Elizabeth Bentley's 'Bill'. 'Bill ' might lead to 'Catherine', who was met by Bentley and is also much wanted.

Lamphere said that the FBI effort on this case, nationwide, was enormous — the work on ALBERT was the most important Venona action then being worked by the Bureau. Also interesting to note are the other Venona cases then working that Lamphere ranked just below ALBERT. These were covernames ALEXANDROV, LILY, and BIBI, none of whom have ever been identified, and covernames OLA (later identified as KGB officer Christina Krotkova) and covername TULIP, who would be identified as Mark Zborowski, a veteran KGB agent who had been involved in the operation to spring Trotsky's murderer from a Mexican prison. We will discuss some of these cases in the next volume. And more from Sudbury:

It is encouraging that the customer [Lamphere] has had more time to devote to our work recently. During the winter [of 1953/54] there have been long periods when it has been impossible for him to visit us because of the almost incredible pressure from above in connection with the Harry Dexter White case. At one stage Lamphere worked every day without a break for five weeks, doing as much as sixty hours of overtime in a single week!

Harry White is, as we will discuss, prominent in Venona. The flap concerned Attorney General Herbert Brownell's public remarks that White had been a traitor and that President Truman had ignored FBI information about him. Ex-President Truman objected and then clarified etc. — Director Hoover, of course, became incensed over comments by Truman and the media. Thus Lamphere was put to work developing a chronology (when the FBI told who — what about Harry White) without directly using the Venona material.

By June 1954, the entire [redacted] party at NSA was working the [redacted] matches, extending the intelligence on KGB operations back into 1943 and even 1942. Chew and VanHouten were even testing the 1941 traffic for matches or within message re-use (not much luck there, however). At that same time Lamphere reported that the FBI had now identified the principal New York signatory, covername MAJ, as Stepan Apresyan, who had arrived at the New York consulate on 21 February 1944, and transferred to San Francisco in March 1945.[26] Lamphere also reported some progress on covername MER/ALBERT, noting that he apparently was a Russian and had been active in the U.S. as far back as 1939.[27]

The U.S. Venona team now began to break up. Katurah McDonald resigned in July 1954. Miss McDonald had been working the problem for 10 years and shares in the credit for some of the cryptanalytic breaks. Her

[24] FP/17, 5 February 1954. The connection was not nearly so close in the UK. The NSA integrees of course had the closest friendly relationship with their Sigint counterparts— but direct contact with Security Service or Secret Service representatives did not take place (except that, during his time at GCHQ as the integree, Gardner did meet with MI–5, at their request, to discuss Philby.)

[25] Of course one can also read through several hundred items that Bob Lamphere gave NSA in support of Venona to appreciate the extraordinary level of his effort.

[26] Up until then, MAJ had been identified as Fedosimov, another member of the New York consulate. Apresian, an Armenian, was obviously a KGB officer in the fast lane. He was only 30 years old when he became the New York Resident, and the Center kept him in the thick of the action. When San Francisco was chosen as the site for the international conference that, among other things, created the UN, Apresian was dispatched to that city.

[27] Covername MER/ALBERT was in fact a Russian — an extraordinarily busy illegal, in fact the Illegal Resident for New York–Washington. We discuss him in Volume two.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

duties were taken up by Janice Cram who had been working Consular material [redacted] for two years.[28] On 20 July 1954, Sudbury reported more news to GCHQ:

> *You will no doubt have heard the sad news that Bob Lamphere has resigned from the FBI. We thus lose the services of a widely experienced counter-espionage specialist who has been working on the [Venona] program since the very early stages.*[29]

(b)(6)
(b)(7)(C)
OGA
FBI

Lamphere's immediate replacements included Ed Tully and [redacted] (who had already been working with him on Venona). As Geoffrey Sudbury recalls, the connection to the FBI changed with Lamphere's departure. As the Venona material continued to age, the Bureau had less and less interest — at least the regular visits came to an end. For example, Howard Vincent (who replaced Sudbury) would note in February 1957, at the time of the arrest of Jack Soble, that, "So far the Bureau has said nothing at all on the part [Venona] played in the arrest of the above mentioned. In fact nothing has been seen of the man from the Bureau since last November. It is hoped that they will come up with some explanation and a morale booster before too long."

From 1955 on the CI analytic support and customer enthusiasm came from Al Kergel of CIA. Some have told me that within the Bureau assignment to the Venona material, at least as a fulltime interest, could not have been seen as career enhancing. The messages were now at least 10 years old (almost nothing after 1945) and the "new" exploitation was pushing the material back in time, not forward, i.e. as mentioned above, 1942 and 1943 material was now being worked, the exploitable (matchable) 1944–1945 messages having mostly been solved and translated. The big cases had been run, or at least the covernames had been extracted and were under investigation. In fact there would be much more to learn from Venona (and for the UK there were indeed many cases still to be worked), though to some extent it became a matter of CI history rather than CI operations. But at the time, in the NSA and GCHQ view, many important breaks still seemed possible.[30]

I. The Later 1950s and early 1960s

A few highlights of those times to bring this volume to a close.

In a February 1957 report to Dr. Sinkov we read that the NSA Venona unit consisted of 12 people directly engaged in exploitation, the GCHQ unit was a bit larger. The division of effort between the two centers was, as always, "very flexible". That report also summarizes the matter of the code books and bookbreaking:

> *The values in both the [redacted] books have been recovered entirely from occurrences in the texts read [bookbreaking without benefit of a code book], while there is a captured copy, partially burned, of the encode version of the [redacted] code. The [redacted] code, [redacted] is still very difficult to read since many of the more useful values are unidentified.*[31]

A GCHQ status report of August 1958, gives us the number of messages that had been matched and the translations issued from same. A total of 3156 KGB messages on all lanes had been matched and 1266 translations issued. The former figure requires some explanation — a match did not mean that a useful text, one worthy of publication, could be obtained. The match, particularly in system [redacted] might never lead to a

[28] Meredith Gardner believes that Miss McDonald did not get the credit due her. He recalls that at her going away luncheon she responded to his speech by telling him that she might not have left if she had realized how important her work was in fact seen by others.
[29] FP/63, Venona Collection.
[30] We will discuss all this in greater detail in Volume two. Lamphere's resignation from the FBI had nothing to do with the status of Venona. We must, of course, be careful in commenting on the FBI's role. It might be best to say that the Bureau continued to work Venona leads with vigor but that the direct liaison (as a full-time job and person-to-person analytic support) declined. Lamphere had been an extraordinary representative.
[31] Handwritten, unsigned reports dated 12 February 1957 in Venona Collection, box D017.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

translation. But of course for the thousands of other KGB (and GRU) messages that were never matched, there was never any possibility of a decryption and translation. The following translations of KGB messages on the U.S. <—> Moscow and Moscow –> London lanes had been issued up to 31 August 1958:

New York	591
San Francisco	84
Washington	12
London	15

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

In addition 36 NY <—> M GRU and 2 Washington <—> Moscow GRU (naval) had been issued. The KGB covername count as of that date went something like this:[32]

	Total #	# Ident.
U.S. <—> Moscow	653	222[33]
Moscow –> London	22	5
Latin Amer. <—> Moscow	123	38

GRU (naval), that is [redacted] now became of interest, as Howard Vincent reported to Bodsworth on 8 September 1958: "In view of the very scant knowledge on the subject of Russian Naval espionage in the USA, CIA has requested a translation of all [redacted] messages however scrappy to see if what is there adds up to anything." In 1959, Bill Kulp, then integrated into the GCHQ Venona party, commented on the [redacted] "Those of us working on the [redacted] material are gratified to see that something of interest to the customers [FBI and CIA] has finally emerged....It is our feeling that the clandestine naval network in the USA was just getting started in 1943 and that later messages will reveal material of more valuable intelligence — we hope!" In fact, only the 1943 material has ever been read, but it is certainly interesting and one wonders how far GRU (naval) was able to proceed in their undercover operations in the U.S.[34]

GCHQ began to consider shutting down or reducing its Venona operation in 1959 (I think this had been considered earlier). Bill Kulp reported to NSA on 20 April that the GCHQ Venona operation:

> *Will continue to operate at its present strength for at least over a year —most likely two years, considering the machine jobs that have been authorized. The British customers were quite persuasive about the value of the material and convinced Alexander and company that as far as they were concerned the stuff was never too old.*[35]

(b)(1)
(b)(3)
OGA

CIA

By the early 1960s, NSA too was considering a reduction in the Venona effort, starting with the withdrawal of the NSA integree at GCHQ. Bodsworth, as head of the GCHQ unit told [redacted] of CIA about NSA's plans. Bodsworth made these points to CIA:

- Venona was still important to the customers and he expected some new breakthroughs, especially in GRU.
- The integration in each center was important to technical progress.

---

[32] [redacted] The Latin American lanes included the heavy and interesting KGB traffic Mexico City < > Moscow (described in Volume two).
[33] This number includes intelligence officers.
[34] Letter from Kulp to Callahan, CFM–16, 20 August 1959 in Venona Collection at 3337, box 13 (in FMC folder).
[35] Kulp to Callahan, 20 April 1959.

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

VIII. VENONA DEVELOPEMENTS DURING THE 1950s

- The assignment of UK people to the NSA Venona effort was much sought after and thus good for morale and professional development.
- The NSA integree at GCHQ received U.S. collateral otherwise unavailable to the UK.[36]

In Volume three we will follow this story of threatened closedowns, and the burst of translations during the final years of the Venona problem. One more point before ending this volume. The entire Venona project, both at GCHQ and NSA, was reinvigorated by the discovery in the 1960s of a new source of traffic — the Swedish collection of KGB and GRU traffic during the 1940–45. This would have three important benefits:

- More traffic for matching purposes
- Traffic on Swedish <—> Moscow lanes
- Traffic on other lanes that had not hitherfore been available, e.g. U.S. <—> Moscow traffic that had fallen into the collection gaps of the early 1940s now became available to some extent from a Swedish cable tap at a terminus of the Great Northern Cable (some NY <—> Moscow traffic, for instance, passed through Sweden).

Howard Vincent has covered this in great detail in his study.

[36] Memo Bill Harvey, CIA, to Dr. Tordella, 25 April 1961 in Venona Collection, 3337, box 13 (Callahan #1).

~~TOP SECRET UMBRA~~

(b)(1)
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36